

# On the MacWilliams Identity for Classical and Quantum Convolutional Codes

Ching-Yi Lai, Min-Hsiu Hsieh, and Hsiao-feng Lu

## Abstract

The usual weight generating functions associating with a convolutional code (CC) are based on state space realizations or the weight adjacency matrices (WAMs). The MacWilliams identity for CCs on the WAMs was first established by Gluesing-Luerssen and Schneider in the case of minimal encoders, and generalized by Forney using the normal factor graph theorem. We define the dual of a convolutional code in the viewpoint of constraint codes and obtain a simple and direct proof of the MacWilliams identity for CCs. By considering the weight enumeration functions over infinite stages, i.e. all codewords of a CC, we establish additional relations between a CC and its dual. Relations between various notions of weight generating function are also clarified, and the reason that no MacWilliams identity exists for free-distance enumerators is clear now. Hence the MacWilliams theorem for CCs can be considered complete. For our purpose, we choose a different representation for the exact weight generating function (EWGF) of a block code, by defining it as a linear combination of orthonormal vectors in Dirac bra-ket notation, rather than the standard polynomial representation. Within this framework, the MacWilliams identity for the EWGFs can be derived with simply a Fourier transform. This representation provides great flexibility so that various notions of weight generating functions and their MacWilliams identities can be easily obtained from the MacWilliams identity for the EWGFs. As a result, we also obtain the MacWilliams identity for the input-output weight adjacency matrices (IOWAMs) of a systematic convolutional code and its dual, which cannot be obtained from previous approaches. Finally, paralleling the development of the classical case, we establish the MacWilliams identity for quantum convolutional codes.

## I. INTRODUCTION

In coding theory, a fundamental theorem is the MacWilliams identity for linear block codes, which provides a precise relation between the weight generating functions of a code and its dual [1]. The weight generating function of a code details the distribution of the codeword weights, which can be used to analyze the error performance of the code. Moreover, the linear programming bounds for linear block codes with constraints from the MacWilliams identities are one of the strongest upper bounds on the size of a code or its minimum distance.<sup>1</sup> It is desired to extend these ideas for CCs.

Convolutional codes offer a rather different coding paradigm. The convolutional structure allows a much lower complexity for encoding and decoding circuits without deteriorating its error-correcting ability [3]. However, it is exactly this convolutional structure that complicates the notions of weight generating functions of CCs. The *free-distance enumerator* is the first such notion that counts the weight distribution of the fundamental paths that start and end in the zero states of a code's state diagram without passing any intermediate zero states [4]. This free-distance enumerator is crucial in the error analysis of a CC; however, it was realized later that the MacWilliams identity does not hold for the free distance enumerators [5]. Evidently an insufficient amount of information about the dual code is contained in the free-distance enumerator.

A more refined notion of a weight generating function is the weight adjacency matrix (WAM) [6], [7], [8]. Each entry of this matrix is the weight distribution of all outputs associated with the corresponding state transitions. Unfortunately, a general WAM strongly depends on the underlining encoder and state space description, and is not an invariant of a CC. However, the WAM is shown to be an invariant of a CC if the encoder is minimal [9]. A breakthrough was made by Gluesing-Luerssen and Schneider in [10], [11], where the MacWilliams identity for the WAMs of a CC and its dual is established. This is mostly because the dependence of WAMs on the state space description can be removed if the *controller canonical form* of the encoders is used. Later, Forney employed the normal graph duality theorem [12] and obtained a more general MacWilliams theorem for various weight generating functions of CCs without the requirement of controller canonical form. Forney's proof of the MacWilliams identity for linear time-invariant CCs is the most general and concise one to date.

This paper outlines a direct proof of the MacWilliams identity for CCs. We first define the EWGF of a linear block code as a linear combination of orthonormal vectors in Dirac bra-ket notation. The EWGFs of a code and its dual are directly related by a Fourier transform operator, which gives exactly the MacWilliams identity for the EWGFs. Various notions of weight generating functions and their MacWilliams identities can be obtained from the MacWilliams identity for the EWGFs [1]. Subsequently, the MacWilliams identity for CCs is derived from the MacWilliams identity for the EWGFs of the *constraint codes* of a CC and its dual. Our proof is inspired by Forney's normal graph duality theorem [13], and does not rely on the controller canonical form. The scalar in the MacWilliams identity for CCs that is missing in [13] is explicitly given in our proof. Moreover, our method provides additional flexibility in defining various notions of weight generating functions

Part of this work will appear in Proceedings of 2014 IEEE Intl. Symp. Inf. Theory.

C.-Y. Lai and M.-H. Hsieh are with the Centre for Quantum Computation & Intelligent Systems, Faculty of Engineering and Information Technology, University of Technology, Sydney, New South Wales, Australia 2007. M.-H. Hsieh is also with the UTS-AMSS Joint Research Laboratory for Quantum Computation and Quantum Information Processing, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China. (emails: ChingYi.Lai@uts.edu.au and Min-Hsiu.Hsieh@uts.edu.au)

H.-F. Lu is with the Department of Electrical and Computer Engineering, at National Chiao Tung University, Taiwan. (email: francis@mail.nctu.edu.tw).

<sup>1</sup>Please refer to code tables in [2] for the best known upper and lower bounds on their minimum distance.

of CCs, including the IOWAMs. As a result, we extend our work to obtain a MacWilliams identity for the IOWAMs of CCs with systematic encoders, and this answers an open question proposed by Gluesing-Luerssen and Schneider [11]. For a nonsystematic encoder, we provide a condition that its IOWAM can be derived from the corresponding systematic encoder. Finally, we propose a weight enumeration function over all codewords of a CC, which will be shown to satisfy a MacWilliams identity. Following that, relations between various weight enumerations in the classical convolutional code literature, including the free-distance enumerators and WAMs, can be illustrated.

Our classical treatment directly paves the way for the establishment of the MacWilliams identity for quantum convolutional codes (QCCs). Quantum coding theory is still in its early stage of development. While the MacWilliams identity for quantum stabilizer codes, the quantum analogue of classical additive block codes, has been proved more than a decade ago [14], [15], [16], the notion of a dual code was defined only very recently [17]. For a quantum stabilizer code defined by a stabilizer group [18], [19], its dual stabilizer code does not exist since the orthogonal group of a stabilizer group is not a stabilizer group. (The notion of orthogonality will be clear after we define an inner product later.) The theory of quantum stabilizer codes is complete after entanglement-assisted quantum error-correcting codes (EAQECCs) were proposed [20], [21] in the sense that the dual code of a stabilizer code is an EAQECC. The MacWilliams identity thus can be established for these codes [17].

QCCs receive great attention for their capabilities in protecting a stream of quantum information in quantum communication, since large blocks of quantum information are very fragile to decoherence [22], [23], [24], [25], [26]. The WAMs and free-distance enumerators of QCCs are defined accordingly and they function like the classical counterparts [27], [28], [29]. We proceed to define the dual code of a QCC within the framework of entanglement-assisted quantum convolutional codes (EA-QCCs) [30], [31], [32]. Similar to the case of quantum stabilizer codes, the dual code of a QCC is an EA-QCC. Our notion of duality coincides with the normal factor graph duality theorem, which details how one can obtain the dual code of a code from its normal realization [12], [13], [33], [34]. Then the MacWilliams identity for EA-QCCs is derived, following the same line as the classical case.

This paper is organized as follows. We introduce the Dirac bra-ket notations and basics of linear block codes and the MacWilliams identity in the next section, so that the materials in this paper are self-complement. In Sec. III, we first discuss classical convolutional codes in the viewpoint of constraints codes and then prove the MacWilliams identities for various notions of weight enumerations of CCs. We summarize the relations of these weight generating functions in Subsec. III-E. The MacWilliams identity for EA-QCCs is given in Sec. IV, as well as the definition of the dual code of an EA-QCC. The conclusion follows in Sec. V.

## II. LINEAR BLOCK CODES

In this section we introduce basic properties of classical error-correcting codes and the MacWilliams identity for linear block codes. We will define the exact weight generating function (EWGF) of a block code as a linear combination of orthonormal vectors in Dirac bra-ket notation. This representation allows us to derive the MacWilliams identity easily. The readers would have a better understanding of the Dirac notation, which is used in both classical and quantum cases throughout this article, if they have never seen it before.

We begin with the Dirac notation. Let  $|\psi\rangle$  be a column vector in a Hilbert space  $\mathcal{V}$ , whose adjoint is denoted by  $\langle\psi| = |\psi\rangle^\dagger$ . Let  $\langle\psi|\phi\rangle$  and  $|\psi\rangle\langle\phi|$  denote the inner product and the outer product of  $|\psi\rangle, |\phi\rangle \in \mathcal{V}$ , respectively. Suppose  $\mathcal{V}$  and  $\mathcal{W}$  are two Hilbert spaces with orthonormal bases  $\{|\psi_j\rangle\}$  and  $\{|\phi_i\rangle\}$ , respectively. If  $A$  is a linear operator from  $\mathcal{V}$  to  $\mathcal{W}$ ,  $A$  can be represented as

$$A = \sum_{i,j} \langle\phi_i|A|\psi_j\rangle |\phi_i\rangle\langle\psi_j|,$$

where  $\langle\phi_i|A|\psi_j\rangle$  is the  $(i, j)$ -th matrix element of  $A$ . The tensor product of an  $s \times t$  matrix  $A = [a_{i,j}]$  and an  $s' \times t'$  matrix  $B$  is defined as

$$A \otimes B = \begin{bmatrix} a_{1,1}B & a_{1,2}B & \cdots & a_{1,t}B \\ a_{2,1}B & a_{2,2}B & \cdots & a_{2,t}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{s,1}B & a_{s,2}B & \cdots & a_{s,t}B \end{bmatrix}.$$

For  $|\psi_1\rangle \in \mathcal{V}_1$  and  $|\psi_2\rangle \in \mathcal{V}_2$ , the tensor product of these two vectors  $|\psi_1\rangle \otimes |\psi_2\rangle$  is a vector in the Hilbert space  $\mathcal{V}_1 \otimes \mathcal{V}_2$ .

Let  $\mathcal{A}_j$  denote a vector space of dimension  $j$  over a finite field  $\mathbb{F}_q$ , where  $q = p^r$  for a prime number  $p$  and a positive integer  $r$ . A classical  $[n, k]$  linear block code  $\mathcal{C}$  over  $\mathbb{F}_q$  is a  $k$ -dimensional subspace of  $\mathcal{A}_n$  with a (full rank)  $(n - k) \times n$  parity-check matrix  $H$  so that for any codeword  $\mathbf{c} \in \mathcal{C}$ ,  $H\mathbf{c}^\top = 0$ , where  $\mathbf{c}^\top$  is the transpose of  $\mathbf{c}$ . The code can also be specified by a (full rank)  $k \times n$  generator matrix  $G$  so that  $\mathcal{C} = \{\mathbf{c} : \mathbf{c} = \mathbf{u}G, \text{ for } \mathbf{u} \in \mathcal{A}_k\}$  and  $GH^\top = 0$ . The dual code  $\mathcal{C}^\perp$  of  $\mathcal{C}$  is the  $[n, n - k]$  linear block code with  $H$  being a generator matrix and  $\mathcal{C}^\perp = \{\mathbf{v} \in \mathcal{A}_n : \mathbf{v} \cdot \mathbf{c} = 0, \forall \mathbf{c} \in \mathcal{C}\}$ , where  $\mathbf{v} \cdot \mathbf{c}$  is the induced inner product of the vector space  $\mathcal{A}_n$ .

Let  $\mathcal{A} \equiv \mathcal{A}_n$ . We define a Hilbert space  $\mathcal{H}_\mathcal{A}$  corresponding to  $\mathcal{A}$  so that for all  $\mathbf{a} \in \mathcal{A}$ ,  $|\mathbf{a}\rangle$  is a vector in  $\mathcal{H}_\mathcal{A}$  and  $\{|\mathbf{a}\rangle\}$  forms an orthonormal basis of  $\mathcal{H}_\mathcal{A}$ . This means that  $\langle\mathbf{a}|\mathbf{a}'\rangle = \delta_{\mathbf{a},\mathbf{a}'}$ , where  $\delta_{\mathbf{a},\mathbf{a}'}$  is the Kronecker delta function. Without loss

of generality, we assume  $\mathcal{A}_1 \equiv \mathbb{F}_q = \{\alpha_0 = 0, \alpha_1, \dots, \alpha_{q-1}\}$  and  $\mathcal{H}_{\mathcal{A}_1}$  is a  $q$ -dimensional Hilbert space with an orthonormal basis  $\{|\alpha_0\rangle, \dots, |\alpha_{q-1}\rangle\}$ . It is obvious that  $\mathcal{H}_{\mathcal{A}} = \mathcal{H}_{\mathcal{A}_1}^{\otimes n}$ , and  $|\mathbf{a}\rangle = |a_1\rangle \otimes \dots \otimes |a_n\rangle$  for  $\mathbf{a} = (a_1 : \dots : a_n) \in \mathcal{A}$  and  $a_i \in \mathcal{A}_1$ . We use the notation  $(\mathbf{a} : \mathbf{b})$  to denote the concatenation of two vectors  $\mathbf{a}$  and  $\mathbf{b}$ .

**Definition 1.** The *exact weight generating function* (EWGF)  $g_{\mathcal{C}}^E$  of a set  $\mathcal{C} \subset \mathcal{A}$  is defined as  $g_{\mathcal{C}}^E = \sum_{\mathbf{c} \in \mathcal{C}} |\mathbf{c}\rangle \in \mathcal{H}_{\mathcal{A}}$ .

We define the EWGF as a linear combination of orthonormal vectors, rather than a multivariate polynomial commonly used in the literature (see, e.g., Ref. [13]). The standard polynomial representation can easily be recovered by a mapping that takes  $|\mathbf{c}\rangle$  to indeterminates  $x(\mathbf{c})$ . It will become clear that this definition leads to an alternative proof of the MacWilliams identities shortly.

Suppose  $\hat{\mathcal{A}}$  is a dual space of  $\mathcal{A}$  of the same dimension that consists of homomorphisms that map  $\mathcal{A}$  to  $\mathbb{F}_p$ . We define a bilinear map  $\langle \hat{\mathbf{a}}, \mathbf{a} \rangle = \hat{\mathbf{a}}(\mathbf{a})$  for  $\hat{\mathbf{a}} \in \hat{\mathcal{A}}$ , and  $\mathbf{a} \in \mathcal{A}$ . The Fourier transform operator  $\mathcal{F}_{\mathcal{A}}$  is defined as

$$\mathcal{F}_{\mathcal{A}} = \sum_{\hat{\mathbf{a}} \in \hat{\mathcal{A}}} \sum_{\mathbf{a} \in \mathcal{A}} \omega^{\langle \hat{\mathbf{a}}, \mathbf{a} \rangle} |\hat{\mathbf{a}}\rangle \langle \mathbf{a}|,$$

where  $\omega = e^{2\pi i/p}$  is a primitive complex  $p$ -th root of unity in  $\mathbb{C}$ . In our discussion of coding theory,  $\hat{\mathcal{A}} = \mathcal{A}$  and  $\langle \hat{\mathbf{a}}, \mathbf{a} \rangle : \mathcal{A} \times \mathcal{A} \rightarrow \mathbb{F}_p$  is the inner product in  $\mathcal{A}$ . Note that  $\mathcal{F}_{\mathcal{A}}^\dagger \mathcal{F}_{\mathcal{A}} = |\mathcal{A}| I^{\otimes n}$ , where  $|\mathcal{A}| = q^n$ . The Fourier transform operator  $\mathcal{F}_{\mathcal{A}}$  has a nice property that it can be decomposed as a tensor product of Fourier transform operators on the components of  $\mathcal{H}_{\mathcal{A}}$ . It is straightforward to verify the following lemma.

**Lemma 2.** Suppose  $n = r + s$ . Then  $\mathcal{H}_{\mathcal{A}} = \mathcal{H}_{\mathcal{A}_r} \otimes \mathcal{H}_{\mathcal{A}_s}$  and

$$\mathcal{F}_{\mathcal{A}} = \mathcal{F}_{\mathcal{A}_r} \otimes \mathcal{F}_{\mathcal{A}_s}.$$

In other words,  $\mathcal{F}_{\mathcal{A}} = \mathcal{F}_{\mathcal{A}_1}^{\otimes n}$ .

Below we prove a MacWilliams identity for EWGFs of a code  $\mathcal{C}$  and its dual.

**Theorem 3.** Suppose  $\mathcal{C}$  is a subspace of  $\mathcal{A}$  with an EWGF  $g_{\mathcal{C}}^E = \sum_{\mathbf{c} \in \mathcal{C}} |\mathbf{c}\rangle$ . The EWGF of its dual space  $\mathcal{C}^\perp$  of  $\mathcal{C}$  with respect to the inner product  $\langle \cdot, \cdot \rangle$  in  $\mathcal{A}$  is

$$g_{\mathcal{C}^\perp}^E = \frac{1}{|\mathcal{C}|} \mathcal{F}_{\mathcal{A}} g_{\mathcal{C}}^E. \quad (1)$$

*Proof:*

$$\begin{aligned} \frac{1}{|\mathcal{C}|} \mathcal{F}_{\mathcal{A}} g_{\mathcal{C}}^E &= \frac{1}{|\mathcal{C}|} \sum_{\hat{\mathbf{a}} \in \hat{\mathcal{A}}} \sum_{\mathbf{a} \in \mathcal{A}} \omega^{\langle \hat{\mathbf{a}}, \mathbf{a} \rangle} |\hat{\mathbf{a}}\rangle \langle \mathbf{a}| \sum_{\mathbf{c} \in \mathcal{C}} |\mathbf{c}\rangle \\ &= \frac{1}{|\mathcal{C}|} \sum_{\hat{\mathbf{a}} \in \hat{\mathcal{A}}} \sum_{\mathbf{c} \in \mathcal{C}} \omega^{\langle \hat{\mathbf{a}}, \mathbf{c} \rangle} |\hat{\mathbf{a}}\rangle \\ &= \sum_{\hat{\mathbf{a}} \in \mathcal{C}^\perp} |\hat{\mathbf{a}}\rangle = g_{\mathcal{C}^\perp}^E, \end{aligned}$$

where the last equality follows from

$$\frac{1}{|\mathcal{C}|} \sum_{\mathbf{c} \in \mathcal{C}} \omega^{\langle \hat{\mathbf{a}}, \mathbf{c} \rangle} = \begin{cases} 1, & \hat{\mathbf{a}} \in \mathcal{C}^\perp; \\ 0, & \hat{\mathbf{a}} \notin \mathcal{C}^\perp. \end{cases}$$

The above equation is obvious for  $\hat{\mathbf{a}} \in \mathcal{C}^\perp$ . For  $\hat{\mathbf{a}} \notin \mathcal{C}^\perp$ , there exists  $\mathbf{c}' \in \mathcal{C}$  such that  $\langle \hat{\mathbf{a}}, \mathbf{c}' \rangle \neq 0$ . Since  $\mathbf{c}' + \mathcal{C} = \mathcal{C}$ , we have  $\sum_{\mathbf{c} \in \mathcal{C}} \omega^{\langle \hat{\mathbf{a}}, \mathbf{c} \rangle} = \sum_{\mathbf{c} \in \mathcal{C}} \omega^{\langle \hat{\mathbf{a}}, \mathbf{c} + \mathbf{c}' \rangle} = \omega^{\langle \hat{\mathbf{a}}, \mathbf{c}' \rangle} \sum_{\mathbf{c} \in \mathcal{C}} \omega^{\langle \hat{\mathbf{a}}, \mathbf{c} \rangle}$ , which implies  $\sum_{\mathbf{c} \in \mathcal{C}} \omega^{\langle \hat{\mathbf{a}}, \mathbf{c} \rangle} = 0$ . ■

The Hamming weight  $\text{wt}(\mathbf{c})$  of a vector  $\mathbf{c}$  is the number of its nonzero components.

**Definition 4.** The *Hamming weight generating function* (HWGF) of  $\mathcal{C}$  is

$$g_{\mathcal{C}}^H(x, y) = \sum_{\mathbf{c} \in \mathcal{C}} x^{n-\text{wt}(\mathbf{c})} y^{\text{wt}(\mathbf{c})} = \sum_{j=0}^n \nu_j x^{n-j} y^j,$$

where  $\nu_j$  is the number of vectors in  $\mathcal{C}$  with Hamming weight  $j$ , and  $x$  and  $y$  are two transcendental numbers over  $\mathbb{C}$ .

We define a linear functional  $\gamma : \mathcal{H}_{\mathcal{A}_1} \rightarrow \mathbb{C}[x, y]$  as

$$\gamma = x\langle 0| + \sum_{a \in \mathcal{A}_1 - \{0\}} y\langle a|. \quad (2)$$

$\gamma$  has a trivial generalization  $\gamma^{\otimes n} : \mathcal{H}_{\mathcal{A}_1}^{\otimes n} \rightarrow \mathbb{C}[x, y]$ . Then the HWGF can be obtained from the EWGF as

$$g_{\mathcal{C}}^H(x, y) = \gamma^{\otimes n} g_{\mathcal{C}}^E.$$

As a consequence, the MacWilliams identity for linear block codes [1] can be obtained by applying  $\gamma^{\otimes n}$  on both sides of (1).

**Corollary 5.** The MacWilliams identity for the HWGFs of a code  $\mathcal{C}$  and its dual is:

$$g_{\mathcal{C}^\perp}^H(x, y) = \frac{1}{|\mathcal{C}|} g_{\mathcal{C}}^H(x + (q-1)y, x - y). \quad (3)$$

*Proof:* Assume  $|v\rangle \in \{|0\rangle, |\alpha_1\rangle, \dots, |\alpha_{q-1}\rangle\}$ . Consider

$$\begin{aligned} \gamma \mathcal{F}_{\mathcal{A}_1} |v\rangle &= \left( x\langle 0| + \sum_{a' \in \mathcal{A}_1 - \{0\}} y\langle a'| \right) \left( \sum_{\hat{a} \in \mathcal{A}_1} \sum_{a \in \mathcal{A}_1} \omega^{\langle \hat{a}, a \rangle} |\hat{a}\rangle \langle a| \right) |v\rangle \\ &= x + \sum_{a' \in \mathcal{A}_1 - \{0\}} \omega^{\langle a', v \rangle} y \\ &= \begin{cases} x + (q-1)y, & \text{if } |v\rangle = |0\rangle, \\ x - y, & \text{otherwise.} \end{cases} \end{aligned}$$

The result naturally follows by Theorem 3 and Lemma 2 as below:

$$\begin{aligned} g_{\mathcal{C}^\perp}^H(x, y) &= \gamma^{\otimes n} g_{\mathcal{C}^\perp}^E \\ &= \frac{1}{|\mathcal{C}|} \gamma^{\otimes n} \mathcal{F}_{\mathcal{A}_1}^{\otimes n} g_{\mathcal{C}}^E \\ &= \frac{1}{|\mathcal{C}|} \sum_{\mathbf{c} \in \mathcal{C}} (x + (q-1)y)^{n-\text{wt}(\mathbf{c})} (x - y)^{\text{wt}(\mathbf{c})} \\ &= \frac{1}{|\mathcal{C}|} g_{\mathcal{C}}^H(x + (q-1)y, x - y). \end{aligned}$$

■

Consider an  $[n, k]$  linear block code  $\mathcal{C}$  over  $\mathbb{F}_q$  with a systematic generator matrix  $G = (I_k \ A)$ . The first  $k$  symbols of a codeword in  $\mathcal{C}$  are the information symbols, while the rest  $n - k$  symbols are parity symbols. We say a codeword  $\mathbf{c} = (\mathbf{c}_I : \mathbf{c}_P) \in \mathcal{C}$ , where  $\mathbf{c}_I \in \mathcal{A}_k$  and  $\mathbf{c}_P \in \mathcal{A}_{n-k}$ , has logical weight  $i$  and parity weight  $o$  if  $\text{wt}(\mathbf{c}_I) = i$  and  $\text{wt}(\mathbf{c}_P) = o$ .

**Definition 6.** The *input-parity weight generating function* (IPWGF) of  $\mathcal{C}$  is

$$g_{\mathcal{C}}^{IP}(x_I, y_I, x_P, y_P) = \sum_{i=0}^k \sum_{o=0}^{n-k} \nu_{i,o} x_I^{k-i} y_I^i x_P^{n-k-o} y_P^o,$$

where  $\nu_{i,o}$  is the number of codewords in  $\mathcal{C}$  with logical weight  $i$  and parity weight  $o$ , and  $x_I, y_I, x_P$  and  $y_P$  are transcendental over  $\mathbb{C}$ .

Similar to  $\gamma$  defined in (2), we define  $\tau_j : \mathcal{H}_{\mathcal{A}_1} \rightarrow \mathbb{C}[u, v]$  as

$$\tau_j = x_j \langle 0| + \sum_{a \in \mathcal{A}_1 - \{0\}} y_j \langle a| \quad (4)$$

for  $j = I, P$ . Then the IPWGF can be obtained from the EWGF as

$$g_{\mathcal{C}}^{IP}(x_I, y_I, x_P, y_P) = (\tau_I^{\otimes k} \otimes \tau_P^{\otimes n-k}) g_{\mathcal{C}}^E.$$

The dual of  $\mathcal{C}$  is the  $[n, n - k]$  linear block code  $\mathcal{C}^\perp$  with a systematic generator matrix  $H = (A^\top \ I_{n-k})$ . In this case, the last  $n - k$  symbols of a codeword in  $\mathcal{C}^\perp$  are the information symbols, while the rest  $k$  symbols are parity symbols.

**Corollary 7.** The MacWilliams identity for the IPWGFs of a code  $\mathcal{C}$  and its dual is as follows:

$$g_{\mathcal{C}^\perp}^{IP}(x_I, y_I, x_P, y_P) = \frac{1}{|\mathcal{C}|} g_{\mathcal{C}}^{IP}(x_P + (q-1)y_P, x_P - y_P, x_I + (q-1)y_I, x_I - y_I). \quad (5)$$

*Proof:* The proof parallels Corollary 5:

$$\begin{aligned}
g_{\mathcal{C}^\perp}^{IP}(x_I, y_I, x_P, y_P) &= (\tau_P^{\otimes k} \otimes \tau_I^{\otimes n-k}) g_{\mathcal{C}^\perp}^E \\
&= \frac{1}{|\mathcal{C}|} (\tau_P^{\otimes k} \otimes \tau_I^{\otimes n-k}) \mathcal{F}_A g_{\mathcal{C}}^E \\
&= \frac{1}{|\mathcal{C}|} g_{\mathcal{C}}^{IP}(x_P + (q-1)y_P, x_P - y_P, x_I + (q-1)y_I, x_I - y_I).
\end{aligned}$$

■

A similar idea is the MacWilliams identity for the *split weight generating functions* of codes of even length obtained by  $|\mathbf{a}|\mathbf{a} + \mathbf{b}|$  construction [1, p. 150]. Following that, a MacWilliams identity for the IPWGFs of a systematic binary linear block code and its dual was proposed in [36], [37].

The results in this section can be directly applied to the quantum case to derive the MacWilliams identities for quantum stabilizer codes with or without entanglement assistance as well [14], [15], [16], [17].

### III. THE MACWILLIAMS IDENTITIES FOR CLASSICAL CONVOLUTIONAL CODES

We devote this section to establishing the MacWilliams identities for various notions of weight generating functions appearing in the literature of classical convolutional coding theory. First, we will investigate the relation between a CC and its dual through the definition of *constraint codes*. The MacWilliams identities for the WAMs and the IOWAMs of CCs can be directly derived from the MacWilliams identity for the constraint codes. Then a *total Hamming weight generating function* that allows us to enumerate all codewords of a CC is proposed. Unlike the free-distance enumerator, a precise duality relation of a CC and its dual can be directly established with respect to the total Hamming weight generating function. Finally, we remark on the relations between the free-distance enumerators and Hamming weight generating functions of a CC and its dual. As a consequence, the reason that no MacWilliams identity exists for the free-distance enumerators is more clear then. The MacWilliams theorem for CCs is summarized in a relations diagram in Fig. 3.

The derivation of the MacWilliams identities for CCs are based on the Dirac notation as in the previous section. For interested readers, we also provide proofs of these identities by the standard polynomial representations in Appendix A.

#### A. The Constraint Codes of Convolutional Codes

Unlike block codes, CCs encode streams of logical information symbols. CCs can be defined by a polynomial matrix, by a scalar matrix, or by a shift register, and these definitions are equivalent [8]. However, we employ the definition of a CC by a *seed transformation matrix*  $T$ , since this seed transformation matrix is directly related to the *constraint code* of a CC. We will show that this definition is equivalent to other definitions by deriving the polynomial generator matrix  $G(D)$  from the seed transformation matrix  $T$ .

Let  $\mathcal{C}$  be an  $(n, k, m)$  convolutional code over  $\mathbb{F}_q$  with a polynomial generator matrix  $G(D) \in \mathbf{M}_{k \times n}(\mathbb{F}_q[D])$  for some indeterminate  $D$  and the overall constraint length  $m$ . Then  $\mathcal{C}$  is a rank- $k$  submodule of  $\mathcal{M} = (\mathbb{F}_q[D])^n$  given by

$$\mathcal{C} = \left\{ \mathbf{u}(D)G(D) : \mathbf{u}(D) \in (\mathbb{F}_q[D])^k \right\}.$$

The dual code  $\mathcal{C}^\perp$  of  $\mathcal{C}$  is defined<sup>2</sup> as

$$\mathcal{C}^\perp := \left\{ \mathbf{c}'(D) \in \mathcal{M} : \mathbf{c}(D)\mathbf{c}'(D^{-1})^\top = 0, \text{ for all } \mathbf{c}(D) \in \mathcal{C} \right\}.$$

An encoder of an  $(n, k, m)$  CC  $\mathcal{C}$  over  $\mathbb{F}_q$  has  $m$  memory symbols and it outputs  $n$  symbols from  $k$  logical input symbols at each time step as shown in Figure 1. Let  $\mathbf{u}_j$  and  $\mathbf{p}_j$  denote the logical input and physical output symbols at time  $j$ , respectively, and let  $\mathbf{w}_j$  and  $\mathbf{w}_{j+1}$  denote the  $m$  memory symbols before and after encoding at time  $j$ , respectively.

**Definition 8.** The seed transformation matrix  $T$  is an  $(m+k) \times (m+n)$  matrix so that

$$(\mathbf{p}_j : \mathbf{w}_{j+1}) = (\mathbf{w}_j : \mathbf{u}_j)T. \quad (6)$$

The Laurent power series representations of CCs are closely related to the seed transformation matrix  $T$ . Suppose  $T = \begin{pmatrix} C & A \\ E & B \end{pmatrix}$ , where  $A, B, C$ , and  $E$  are  $m \times m, k \times m, m \times n$ , and  $k \times n$  matrices over  $\mathbb{F}_q$ , respectively. By (6),  $(A, B, C, E)$  satisfies

$$\begin{aligned}
\mathbf{w}_{j+1} &= \mathbf{w}_j A + \mathbf{u}_j B \\
\mathbf{p}_j &= \mathbf{w}_j C + \mathbf{u}_j E,
\end{aligned}$$

<sup>2</sup>In [11], their duality is defined by  $G(D)H(D)^\top = 0$ . However, we prefer to define the dual of a convolutional code by  $G(D)H(D^{-1})^\top = 0$  and here is the reason: Consider two polynomials  $g(D) = \sum_i g_i D^i$  and  $h(D) = \sum_j h_j D^j \in \mathbb{F}_q[D]$ . Observe that the constant term of  $g(D)h(D^{-1})$  is  $\sum_i g_i h_i$ . Therefore, the code space generated by  $g(D)$  is orthogonal to that generated by  $h(D)$  if  $g(D)h(D^{-1}) = 0$ . This may explain the additional transpose on the WAM in their formula for MacWilliams identity in [11]. Also, our results coincide with Forney's [13].

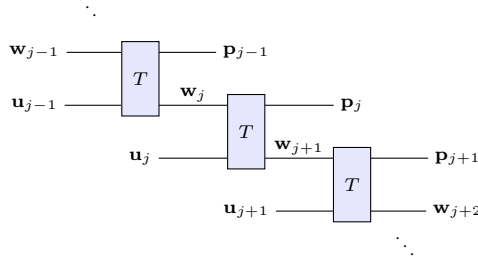


Fig. 1. Circuit diagram of a convolutional encoder with a seed transformation matrix  $T$ .

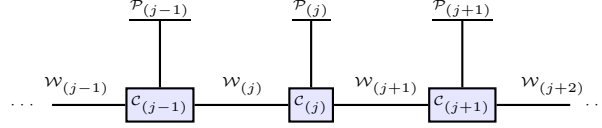


Fig. 2. The normal graph of a conventional state realization.

and is a realization of an encoder of  $\mathcal{C}$ . It is well known that

$$G(D) = B(D^{-1}I_m - A)^{-1}C + E, \quad (7)$$

where  $I_m$  is the  $m \times m$  identity matrix (see, e.g., [35], [9]).

Before we show how to obtain the MacWilliams identity for CCs, we introduce the idea of *constraint codes*, which can be used to define the dual code of a CC according to the normal graph duality theorem [13]. We then show that the MacWilliams identity for CCs can be derived from the MacWilliams identity for the constraint code and its dual.

The normal graph of the state realization of an  $(n, k, m)$  CC  $\mathcal{C}$  is shown in Fig. 2, where  $\mathcal{W}_{(j)} \equiv \mathcal{A}_m$  denotes the input memory space and  $\mathcal{P}_{(j)} \equiv \mathcal{A}_n$  is the output space of  $\mathcal{C}$  at time  $j$ . (For more details about normal graph theorem, please refer to [13].)

**Definition 9.** The *constraint codes*  $\mathcal{C}_{(j)}$  of  $\mathcal{C}$  are  $[2m + n, m + k]$  linear block codes over  $\mathbb{F}_q$  given by

$$\mathcal{C}_{(j)} = \{(\mathbf{w}_j : \mathbf{p}_j : \mathbf{w}_{j+1}) \in \mathcal{A}_{n+2m} : (\mathbf{p}_j : \mathbf{w}_{j+1}) = (\mathbf{w}_j : \mathbf{u}_j)T, \text{ for } \mathbf{u}_j \in \mathcal{A}_k\},$$

where  $T = \begin{pmatrix} C & A \\ E & B \end{pmatrix}$  is the seed transformation matrix of  $\mathcal{C}$ . Alternatively, the constraint code  $\mathcal{C}_{(j)}$  has a generator matrix

$$\tilde{G} = \left( \begin{array}{c|cc} I_m & C & A \\ \hline 0 & E & B \end{array} \right). \quad (8)$$

From the normal factor graph duality theorem for linear codes [13], we have the following definition for the dual of a CC.

**Definition 10.** The  $[2m + n, m + n - k]$  constraint code  $\hat{\mathcal{C}}_{(j)}$  of the dual convolutional code  $\mathcal{C}^\perp$  of  $\mathcal{C}$  is

$$\hat{\mathcal{C}}_{(j)} = \{(\mathbf{w}'_j : \mathbf{p}'_j : \mathbf{w}'_{j+1}) \in \mathcal{A}_{2m+n} : \mathbf{w}'_j \mathbf{w}_j^\top + \mathbf{p}'_j \mathbf{p}_j^\top - \mathbf{w}'_{j+1} \mathbf{w}_{j+1} = 0, \text{ for all } (\mathbf{w}_j : \mathbf{p}_j : \mathbf{w}_{j+1}) \in \mathcal{C}_{(j)}\}.$$

In other words,  $\hat{\mathcal{C}}_{(j)}$  has an  $(m + n - k) \times (2m + n)$  generator matrix  $\tilde{H}$  so that  $\tilde{H}' = \tilde{H} \cdot \text{diag}(I_m, I_n, -I_m)$  is a parity-check matrix of  $\mathcal{C}_{(j)}$ , where

$$\text{diag}(A_1, A_2, \dots) := \begin{pmatrix} A_1 & & \\ & A_2 & \\ & & \ddots \end{pmatrix}.$$

It can be verified that the linear block code defined by the generator matrix  $\tilde{H}$  in Definition 10 is indeed the constraint code of the dual convolutional code  $\mathcal{C}^\perp$  of  $\mathcal{C}$ . Suppose  $G(D)$  and  $H(D)$  are the polynomial generator matrices of  $\mathcal{C}$  and  $\mathcal{C}^\perp$ , respectively. Let  $\tilde{H} = \left( \begin{array}{c|cc} I_m & C' & A' \\ \hline 0 & E' & B' \end{array} \right)$  and  $\tilde{G}$  be as given in (8). As in (7), the polynomial generator matrix of  $\mathcal{C}^\perp$  is

$H(D) = B'(D^{-1}I_m - A')^{-1}C' + E'$ . Since  $\tilde{G}\tilde{H}'^\top = 0$ , we have

$$I_m + CC'^\top - AA'^\top = 0 \quad (9)$$

$$EE'^\top - BB'^\top = 0 \quad (10)$$

$$CE'^\top - AB'^\top = 0 \quad (11)$$

$$EC'^\top - BA'^\top = 0. \quad (12)$$

Then we can show that  $G(D)H(D^{-1})^\top = 0$  as follows:

$$\begin{aligned} G(D)H(D^{-1})^\top &= (B(D^{-1}I_m - A)^{-1}C + E) (B'(DI_m - A')^{-1}C' + E')^\top \\ &\stackrel{(a)}{=} B((D^{-1}I_m - A)^{-1}CC'^\top((DI_m - A')^{-1})^\top + (D^{-1}I_m - A)^{-1}A + A'^\top((DI_m - A')^{-1})^\top + I_m) B'^\top \\ &\stackrel{(b)}{=} B((D^{-1}I_m - A)^{-1}AA'^\top((DI_m - A')^{-1})^\top + (D^{-1}I_m - A)^{-1}A \\ &\quad + A'^\top((DI_m - A')^{-1})^\top + I_m - (D^{-1}I_m - A)^{-1}((DI_m - A')^{-1})^\top) B'^\top \\ &\stackrel{(c)}{=} 0, \end{aligned}$$

where (a) follows from (10), (11), and (12); (b) follows from (9); (c) is obtained by sequentially applying the following two equalities:

$$\begin{aligned} I_m + (D^{-1}I_m - A)^{-1}A &= D^{-1}(D^{-1}I_m - A)^{-1} \\ I_m + A'^\top((DI_m - A')^{-1})^\top &= D((DI_m - A')^{-1})^\top. \end{aligned}$$

Herein, we clarify the notations of  $\hat{\mathcal{C}}_{(j)}$  and  $\mathcal{C}_{(j)}^\perp$ . We denote by  $\hat{\mathcal{C}}_{(j)}$  the constraint code of the dual CC  $\mathcal{C}^\perp$ , and denote by  $\mathcal{C}_{(j)}^\perp$  the dual of the constraint code  $\mathcal{C}_{(j)}$  of  $\mathcal{C}$ . Specifically, if  $(\mathbf{w}_j : \mathbf{p}_j : \mathbf{w}_{j+1}) = (\mathbf{w}_j : \mathbf{u}_j)\tilde{H}$  is a codeword of  $\hat{\mathcal{C}}_{(j)}$  for some  $\mathbf{u}_j \in \mathcal{A}_{n-k}$ , then  $(\mathbf{w}_j : \mathbf{p}_j : -\mathbf{w}_{j+1})$  is a codeword of  $\mathcal{C}_{(j)}^\perp$  by Definition 10.

**Lemma 11.** The EWGF  $g_{\hat{\mathcal{C}}_{(j)}}^E$  of the constraint code  $\hat{\mathcal{C}}_{(j)}$  is related to the EWGF  $g_{\mathcal{C}_{(j)}^\perp}^E$  of  $\mathcal{C}_{(j)}^\perp$  by

$$g_{\hat{\mathcal{C}}_{(j)}}^E = (I^{\otimes m+n} \otimes \Pi) g_{\mathcal{C}_{(j)}^\perp}^E,$$

where  $\Pi = \sum_{\mathbf{w} \in \mathcal{A}_m} |\mathbf{w}\rangle \langle -\mathbf{w}|$  is a permutation on the  $m$  memory symbol states and  $I^{\otimes m+n}$  is the identity operator on the first  $m+n$  symbol states.

Note that in the case that  $q$  is a power of 2,  $\Pi$  is trivial and we have  $\hat{\mathcal{C}}_{(j)} = \mathcal{C}_{(j)}^\perp$ .

### B. The MacWilliams Identity for Convolutional Codes

The weight adjacency matrices of  $\mathcal{C}$  are weight enumeration of the constraint codes  $\mathcal{C}_{(j)}$  in matrix form.

**Definition 12.** The *weight adjacency matrix* (WAM)  $\Lambda_{\mathcal{C}_{(j)}}(x, y)$  of a CC with a constraint code  $\mathcal{C}_{(j)}$  is the matrix whose  $(\mathbf{w}_j, \mathbf{w}_{j+1})$  entry is a HWGF of the output symbols of  $\mathcal{C}_{(j)}$  with the memory symbols before and after time  $j$  being  $\mathbf{w}_j$  and  $\mathbf{w}_{j+1}$ , respectively. That is,

$$\begin{aligned} \langle \mathbf{w}_j | \Lambda_{\mathcal{C}_{(j)}}(x, y) | \mathbf{w}_{j+1} \rangle &\equiv (\langle \mathbf{w}_j | \otimes \gamma^{\otimes n} \otimes \langle \mathbf{w}_{j+1} |) g_{\mathcal{C}_{(j)}}^E \\ &= \gamma^{\otimes n} \left( \sum_{\substack{\mathbf{p}_j \in \mathcal{P}_{(j)}: \\ (\mathbf{w}_j : \mathbf{p}_j : \mathbf{w}_{j+1}) \in \mathcal{C}_{(j)}}} |\mathbf{p}_j\rangle \right). \end{aligned}$$

Now we are ready to derive the MacWilliams identity for convolutional codes [10], [11], [13].

**Theorem 13.** Suppose the WAM of an  $(n, k, m)$  CC  $\mathcal{C}$  over  $\mathbb{F}_q$  is  $\Lambda_{\mathcal{C}_{(j)}}(x, y)$ . Then the WAM for  $\hat{\mathcal{C}}_{(j)}$  is given by

$$\Lambda_{\hat{\mathcal{C}}_{(j)}}(x, y) = \frac{1}{q^{m+k}} \mathcal{F}_{\mathcal{A}_m} \Lambda_{\mathcal{C}_{(j)}}(x + (q-1)y, x-y) \mathcal{F}_{\mathcal{A}_m}^\dagger. \quad (13)$$

*Proof:* From Lemma 11,

$$\begin{aligned}
g_{\hat{\mathcal{C}}_{(j)}}^E &= (I^{\otimes m+n} \otimes \Pi) g_{\mathcal{C}_{(j)}}^E \\
&= \frac{1}{q^{m+k}} (I^{\otimes m+n} \otimes \Pi) \mathcal{F}_{\mathcal{A}_{2m+n}} g_{\mathcal{C}_{(j)}}^E \\
&= \frac{1}{q^{m+k}} \sum_{\mathbf{w}_j \in \mathcal{W}_{(j)}} \sum_{\mathbf{w}_{j+1} \in \mathcal{W}_{(j+1)}} \sum_{\substack{\mathbf{p}_j \in \mathcal{P}_{(j)}: \\ (\mathbf{w}_j, \mathbf{p}_j, \mathbf{w}_{j+1}) \in \mathcal{C}_{(j)}}} (\mathcal{F}_{\mathcal{A}_m} |\mathbf{w}_j\rangle) (\mathcal{F}_{\mathcal{A}_n} |\mathbf{p}_j\rangle) (\Pi \mathcal{F}_{\mathcal{A}_m} |\mathbf{w}_{j+1}\rangle),
\end{aligned}$$

where the second equality follows from Theorem 3 and the last equality is from Lemma 2. Thus

$$\begin{aligned}
\langle \mathbf{w}'_j | \Lambda_{\hat{\mathcal{C}}_{(j)}}(x, y) | \mathbf{w}'_{j+1} \rangle &= (\langle \mathbf{w}'_j | \otimes \gamma^{\otimes n} \otimes \langle \mathbf{w}'_{j+1} |) g_{\hat{\mathcal{C}}_{(j)}}^E \\
&= \frac{1}{q^{m+k}} \sum_{\mathbf{w}_j} \sum_{\mathbf{w}_{j+1}} \sum_{\substack{\mathbf{p}_j \in \mathcal{P}_{(j)}: \\ (\mathbf{w}_j, \mathbf{p}_j, \mathbf{w}_{j+1}) \in \mathcal{C}_{(j)}}} (\langle \mathbf{w}'_j | \mathcal{F}_{\mathcal{A}_m} | \mathbf{w}_j \rangle) (\gamma^{\otimes n} \mathcal{F}_{\mathcal{A}_n} | \mathbf{p}_j \rangle) (\langle \mathbf{w}'_{j+1} | \Pi \mathcal{F}_{\mathcal{A}_m} | \mathbf{w}_{j+1} \rangle) \\
&= \frac{1}{q^{m+k}} \sum_{\mathbf{w}_j} \sum_{\mathbf{w}_{j+1}} \langle \mathbf{w}'_j | \mathcal{F}_{\mathcal{A}_m} | \mathbf{w}_j \rangle \left( \sum_{\substack{\mathbf{p}_j \in \mathcal{P}_{(j)}: \\ (\mathbf{w}_j, \mathbf{p}_j, \mathbf{w}_{j+1}) \in \mathcal{C}_{(j)}}} \gamma^{\otimes n} \mathcal{F}_{\mathcal{A}_n} | \mathbf{p}_j \rangle \right) \langle \mathbf{w}'_{j+1} | \Pi \mathcal{F}_{\mathcal{A}_m} | \mathbf{w}_{j+1} \rangle \\
&\stackrel{(a)}{=} \frac{1}{q^{m+k}} \sum_{\mathbf{w}_j} \sum_{\mathbf{w}_{j+1}} \langle \mathbf{w}'_j | \mathcal{F}_{\mathcal{A}_m} | \mathbf{w}_j \rangle \langle \mathbf{w}_j | \Lambda_{\mathcal{C}_{(j)}}(x + (q-1)y, x-y) | \mathbf{w}_{j+1} \rangle \langle \mathbf{w}_{j+1} | \mathcal{F}_{\mathcal{A}_m}^\dagger | \mathbf{w}'_{j+1} \rangle \\
&\stackrel{(b)}{=} \frac{1}{q^{m+k}} \langle \mathbf{w}'_j | \mathcal{F}_{\mathcal{A}_m} \Lambda_{\mathcal{C}_{(j)}}(x + (q-1)y, x-y) \mathcal{F}_{\mathcal{A}_m}^\dagger | \mathbf{w}'_{j+1} \rangle,
\end{aligned}$$

where (a) follows from the definition of  $\Lambda_{\mathcal{C}_{(j)}}(x, y)$  and  $\langle \mathbf{w}'_{j+1} | \Pi \mathcal{F}_{\mathcal{A}_m} | \mathbf{w}_{j+1} \rangle = \langle \mathbf{w}_{j+1} | \mathcal{F}_{\mathcal{A}_m}^\dagger | \mathbf{w}'_{j+1} \rangle$ ; (b) follows from  $\sum_{\mathbf{w}_j} |\mathbf{w}_j\rangle \langle \mathbf{w}_j| = \sum_{\mathbf{w}_{j+1}} |\mathbf{w}_{j+1}\rangle \langle \mathbf{w}_{j+1}| = I^{\otimes m}$ . We verify  $\langle \mathbf{w}'_{j+1} | \Pi \mathcal{F}_{\mathcal{A}_m} | \mathbf{w}_{j+1} \rangle = \langle \mathbf{w}_{j+1} | \mathcal{F}_{\mathcal{A}_m}^\dagger | \mathbf{w}'_{j+1} \rangle$  as follows:

$$\begin{aligned}
\langle \mathbf{w}'_{j+1} | \Pi \mathcal{F}_{\mathcal{A}_m} | \mathbf{w}_{j+1} \rangle &= \langle \mathbf{w}'_{j+1} | \Pi \left( \sum_{\hat{\mathbf{a}}, \mathbf{a}} \omega^{\langle \hat{\mathbf{a}}, \mathbf{a} \rangle} | \hat{\mathbf{a}} \rangle \langle \mathbf{a} | \right) | \mathbf{w}_{j+1} \rangle \\
&= \sum_{\hat{\mathbf{a}}, \mathbf{a}} \omega^{\langle \hat{\mathbf{a}}, \mathbf{a} \rangle} \langle \mathbf{w}'_{j+1} | - \hat{\mathbf{a}} \rangle \langle \mathbf{a} | \mathbf{w}_{j+1} \rangle \\
&= \sum_{\hat{\mathbf{a}}, \mathbf{a}} \omega^{-\langle \hat{\mathbf{a}}, \mathbf{a} \rangle} \langle \mathbf{w}_{j+1} | \mathbf{a} \rangle \langle \hat{\mathbf{a}} | \mathbf{w}'_{j+1} \rangle \\
&= \langle \mathbf{w}_{j+1} | \sum_{\hat{\mathbf{a}}, \mathbf{a}} \omega^{-\langle \hat{\mathbf{a}}, \mathbf{a} \rangle} | \mathbf{a} \rangle \langle \hat{\mathbf{a}} | \mathbf{w}'_{j+1} \rangle \\
&= \langle \mathbf{w}_{j+1} | \mathcal{F}_{\mathcal{A}_m}^\dagger | \mathbf{w}'_{j+1} \rangle.
\end{aligned}$$

Consequently, we have

$$\Lambda_{\hat{\mathcal{C}}_{(j)}}(x, y) = \frac{1}{q^{m+k}} \mathcal{F}_{\mathcal{A}_m} \Lambda_{\mathcal{C}_{(j)}}(x + (q-1)y, x-y) \mathcal{F}_{\mathcal{A}_m}^\dagger.$$

■

Finally, we remark on the uniqueness of the MacWilliams identity in Theorem 13. While different generator matrices of a constraint code lead to different encoders of a CC, they generate the same code space of the constraint code. Since the MacWilliams identity for CCs is derived from the MacWilliams identity for their constraint codes, this identity is unique for a CC defined by the constraint codes. It can be seen that the encoder need not be minimal in our proof of the MacWilliams identity for CCs. Thus we have provided a simpler proof than that in [10], [11] where the *control canonical form* of a minimal encoder of  $\mathcal{C}$  is necessary. Also, this direct proof gives the scalar in the MacWilliams identity for CCs that is missing in [13].

### C. The MacWilliams Identity for the Input-Output Weight Adjacency Matrices of Convolutional Codes

In this subsection, we extend our work to the IOWAMs of CCs. As Gluesing-Luerssen and Schneider noted in [11], these weight generating functions are not invariants of a CC, but rather of the encoder. We will derive the MacWilliams identity for IOWAMs of a CC and its dual with systematic encoders. In addition, we show the IOWAM of a special type of nonsystematic encoder can be derived from that of its systematic encoder when the entries are monomials. The general form of the MacWilliams identity for IOWAMs needs further investigation.



Recall that a seed transformation matrix of an  $(n, k, m)$  convolutional code  $\mathcal{C}$  is of the form  $T = \begin{pmatrix} C & A \\ E & B \end{pmatrix}$  and it defines the constraint code with a generator matrix  $\tilde{G}$  given in (8). Here we consider the seed transformation matrix of a *systematic encoder*, that is, the matrices  $C$  and  $E$  are in the following specific form:

$$\begin{pmatrix} C \\ E \end{pmatrix} = \begin{pmatrix} 0 & C_0 \\ I_k & E_0 \end{pmatrix}$$

where  $C_0$  and  $E_0$  are  $m \times (n - k)$  and  $k \times (n - k)$  matrices, respectively. We may assume the generator matrix  $\tilde{G}_S$  of the constraint code corresponding to a systematic encoder is

$$\tilde{G}_S = \left( \begin{array}{c|c|c|c} I_m & 0 & C_0 & A_0 \\ \hline 0 & I_k & E_0 & B_0 \end{array} \right). \quad (14)$$

Thus  $(\mathbf{w}_j, \mathbf{p}_j, \mathbf{w}_{j+1})$  is a codeword of  $\mathcal{C}_{(j)}$  for  $\mathbf{u}_j \in \mathcal{A}_k$  if

$$\begin{aligned} \mathbf{w}_{j+1} &= \mathbf{w}_j A_0 + \mathbf{u}_j B_0, \\ \mathbf{p}_j &= (\mathbf{u}_j : \mathbf{w}_j C_0 + \mathbf{u}_j E_0) \triangleq \mathbf{p}^I : \mathbf{p}^P, \end{aligned}$$

where  $\mathbf{p}^I = \mathbf{u}_j$  and  $\mathbf{p}^P = \mathbf{w}_j C_0 + \mathbf{u}_j E_0$ .

**Definition 14.** The input-parity weight adjacency matrix (IPWAM) of a *systematic* convolutional encoder  $\tilde{G}_S$  is the matrix  $\Lambda_{\mathcal{C}_{(j)}}(x_I, y_I, x_P, y_P)$  whose  $(\mathbf{w}_j, \mathbf{w}_{j+1})$  entry is an IPWGF of  $\mathcal{C}_{(j)}$  in  $x_I, y_I, x_P$ , and  $y_P$  by  $\sum_{i,o} \nu_{i,o} x_I^{k-i} y_I^i x_P^{n-k-o} y_P^o$ , where  $\nu_{i,o}$  is the number of  $\mathbf{p}_j = \mathbf{p}^I : \mathbf{p}^P \in \mathcal{A}_n$  with  $\text{wt}(\mathbf{p}^I) = i$  and  $\text{wt}(\mathbf{p}^P) = o$  so that  $(\mathbf{w}_j : \mathbf{p}^I : \mathbf{p}^P : \mathbf{w}_{j+1}) \in \mathcal{C}_{(j)}$ . That is,

$$\langle \mathbf{w}_j | \Lambda_{\mathcal{C}_{(j)}}(x_I, y_I, x_P, y_P) | \mathbf{w}_{j+1} \rangle = \sum_{\substack{\mathbf{p}_j \in \mathcal{P}_{(j)}: \\ (\mathbf{w}_j : \mathbf{p}_j : \mathbf{w}_{j+1}) \in \mathcal{C}_{(j)}}} \tau_I^{\otimes k} \otimes \tau_P^{\otimes n-k} | \mathbf{p}_j \rangle,$$

where  $\tau_j$  are defined in (4).

We slightly abuse the notation  $\Lambda_{\mathcal{C}_{(j)}}$  with regular WAMs; though, there should be no ambiguity from the context and  $\Lambda_{\mathcal{C}_{(j)}}(x, y) = \Lambda_{\mathcal{C}_{(j)}}(x, y, x, y)$  for a systematic encoder.

For simplicity, we assume the corresponding systematic encoder  $\tilde{H}_S$  for the constraint code  $\hat{\mathcal{C}}_{(j)}$  of  $\mathcal{C}^\perp$  is of the form

$$\tilde{H}_S = \left( \begin{array}{c|c|c|c} I_m & C'_0 & 0 & A'_0 \\ \hline 0 & E'_0 & I_{n-k} & B'_0 \end{array} \right).$$

Thus  $(\mathbf{w}_j, \mathbf{p}_j, \mathbf{w}_{j+1})$  is a codeword of  $\hat{\mathcal{C}}_{(j)}$  for  $\mathbf{u}_j \in \mathcal{A}_{n-k}$  if

$$\begin{aligned} \mathbf{w}_{j+1} &= \mathbf{w}_j A'_0 + \mathbf{u}_j B'_0, \\ \mathbf{p}_j &= (\mathbf{w}_j C'_0 + \mathbf{u}_j E'_0 : \mathbf{u}_j) \triangleq \mathbf{p}^P : \mathbf{p}^I. \end{aligned}$$

where  $\mathbf{p}^I = \mathbf{u}_j$  and  $\mathbf{p}^P = \mathbf{w}_j C'_0 + \mathbf{u}_j E'_0$ .

Similarly to the previous development, it is straightforward to have the following MacWilliams identity for the IPWAMs of a systematic encoder of  $\mathcal{C}$  and its dual.

**Theorem 15.** Suppose the IPWAM of a systematic encoder of an  $(n, k, m)$  CC  $\mathcal{C}$  over  $\mathbb{F}_q$  is  $\Lambda_{\mathcal{C}_{(j)}}(x_I, y_I, x_P, y_P)$ . Then the IPWAM of its dual encoder of  $\mathcal{C}^\perp$  is

$$\Lambda_{\hat{\mathcal{C}}_{(j)}}(x_I, y_I, x_P, y_P) = \frac{1}{q^{m+k}} \mathcal{F}_{\mathcal{A}_m} \Lambda_{\mathcal{C}_{(j)}}(x_P + (q-1)y_P, x_P - y_P, x_I + (q-1)y_I, x_I - y_I) \mathcal{F}_{\mathcal{A}_m}^\dagger, \quad (15)$$

where  $\Pi = \sum_{\mathbf{w} \in \mathcal{A}_m} |\mathbf{w}\rangle \langle -\mathbf{w}|$ .

*Proof:* The proof can be completed in a similar fashion to Theorem 13. ■

Remark: Given the systematic encoder  $\tilde{G}_S$  of  $\mathcal{C}$  in (14), it may be natural to define the corresponding systematic encoder  $\tilde{H}_S$  for the constraint code  $\hat{\mathcal{C}}_{(j)}$  of  $\mathcal{C}^\perp$  as

$$\tilde{H}_S = \left( \begin{array}{c|c|c|c} C_0^T & E_0^T & I_{n-k} & 0 \\ \hline A_0^T & B_0^T & 0 & -I_m \end{array} \right).$$

Then a codeword of  $\hat{\mathcal{C}}_{(j)}$  is in the reverse order  $(\mathbf{w}_{j+1} : \mathbf{p}_j : \mathbf{w}_j) = (\mathbf{w}_{j+1} : \mathbf{p}^P : \mathbf{p}^I : \mathbf{w}_j)$ . The MacWilliams identity for the IPWAMs in the above theorem still holds, except that  $\Lambda_{\mathcal{C}_{(j)}}(x_I, y_I, x_P, y_P)$  is replaced with  $\Lambda_{\hat{\mathcal{C}}_{(j)}}^\top(x_I, y_I, x_P, y_P)$  in (15).

However, this identity for CCs would require the duality  $G(D)H(D)^\top = 0$ , which is inconsistent with our development.

Apparently Definition 14 does not apply to nonsystematic encoders. Thus we have the following definition.

**Definition 16.** The IOWAM  $\Delta_{\mathcal{C}_{(j)}}^{\tilde{G}}(x_I, y_I, x_O, y_O)$  of a convolutional encoder  $\tilde{G}$  is the matrix whose  $(\mathbf{w}_j, \mathbf{w}_{j+1})$  entry is a weight generating function in  $x_I, y_I, x_O$ , and  $y_O$  by  $\sum_{i,o} \nu_{i,o} x_I^{k-i} y_I^i x_O^{n-o} y_O^o$ , where  $\nu_{i,o}$  is the number of  $\mathbf{p}_j \in \mathcal{P}_{(j)}$  so that  $(\mathbf{w}_j : \mathbf{p}_j : \mathbf{w}_{j+1}) = (\mathbf{w}_j : \mathbf{u}_j) \tilde{G} \in \mathcal{C}_{(j)}$  with  $\text{wt}(\mathbf{u}_j) = i$  and  $\text{wt}(\mathbf{p}_j) = o$ .

In particular,  $\Delta_{\mathcal{C}_{(j)}}^{\tilde{G}_S}(x_I, y_I, x_O, y_O) = \Lambda_{\mathcal{C}_{(j)}}(x_I x_O, y_I y_O, x_O, y_O)$  for a systematic encoder  $\tilde{G}_S$ , and  $\Lambda_{\mathcal{C}_{(j)}}(x, y) = \Delta_{\mathcal{C}_{(j)}}^{\tilde{G}}(1, 1, x, y)$  for any  $\tilde{G}$  since  $\Lambda_{\mathcal{C}_{(j)}}(x, y)$  is an invariant of the constraint code. The MacWilliams identity for these IOWAMs of systematic encoders directly follows from Theorem 15.

Unlike an IOWAM of a systematic encoder, the IOWAM of a nonsystematic encoder cannot be obtained directly from the EWGF of its constraint code. Below we show that  $\Delta_{\mathcal{C}_{(j)}}^{\tilde{G}}(x_I, y_I, x_O, y_O)$  of a nonsystematic encoder  $\tilde{G}$  can be obtained from  $\Delta_{\mathcal{C}_{(j)}}^{\tilde{G}_S}(x_I, y_I, x_O, y_O)$  when the entries of  $\Delta_{\mathcal{C}_{(j)}}^{\tilde{G}}(x_I, y_I, x_O, y_O)$  are monomials.

Without loss of generality, a nonsystematic generator matrix  $\tilde{G}$  for the constraint code can be expressed as

$$\tilde{G} = \left( \begin{array}{c|cc} I_m & F & C_0 + FE_0 \\ \hline 0 & L & LE_0 \end{array} \middle| \begin{array}{c} A_0 + FB_0 \\ LB_0 \end{array} \right), \quad (16)$$

where  $A_0, B_0, C_0, E_0$  are the matrices given in (14), and  $F, L$  are  $m \times k$  and  $k \times k$  matrices, respectively.

**Theorem 17.** Consider  $\tilde{G}$  given in (16). If  $L = I_k$  and the entries of  $\Delta_{\mathcal{C}_{(j)}}^{\tilde{G}}(x_I, y_I, x_O, y_O)$  are monomials, then its  $(\mathbf{w}_j, \mathbf{w}_{j+1})$  entry is

$$\langle \mathbf{w}_j | \Delta_{\mathcal{C}_{(j)}}^{\tilde{G}}(x_I, y_I, x_O, y_O) | \mathbf{w}_{j+1} \rangle = \langle \mathbf{w}_j | \Delta_{\mathcal{C}_{(j)}}^{\tilde{G}_S}(x_I, y_I, 1, 1) | \mathbf{w}_{j+1} - \mathbf{w}_j F B_0 \rangle \langle \mathbf{w}_j | \Lambda_{\mathcal{C}_{(j)}}(x_O, y_O) | \mathbf{w}_{j+1} \rangle.$$

*Proof:* By assumption, each entry of  $\Delta_{\mathcal{C}_{(j)}}^{\tilde{G}}(x_I, y_I, x_O, y_O)$  is a monomial in  $x_I, y_I, x_O$ , and  $y_O$ , and we have

$$\langle \mathbf{w}_j | \Delta_{\mathcal{C}_{(j)}}^{\tilde{G}}(x_I, y_I, x_O, y_O) | \mathbf{w}_{j+1} \rangle = \langle \mathbf{w}_j | \Delta_{\mathcal{C}_{(j)}}^{\tilde{G}}(x_I, y_I, 1, 1) | \mathbf{w}_{j+1} \rangle \langle \mathbf{w}_j | \Delta_{\mathcal{C}_{(j)}}^{\tilde{G}}(1, 1, x_O, y_O) | \mathbf{w}_{j+1} \rangle.$$

Since  $\Lambda_{\mathcal{C}_{(j)}}(x, y)$  is an invariant of the constraint code, we have

$$\langle \mathbf{w}_j | \Delta_{\mathcal{C}_{(j)}}^{\tilde{G}}(1, 1, x_O, y_O) | \mathbf{w}_{j+1} \rangle = \langle \mathbf{w}_j | \Lambda_{\mathcal{C}_{(j)}}(x_O, y_O) | \mathbf{w}_{j+1} \rangle,$$

It remains to show that  $\langle \mathbf{w}_j | \Delta_{\mathcal{C}_{(j)}}^{\tilde{G}}(x_I, y_I, 1, 1) | \mathbf{w}_{j+1} \rangle = \langle \mathbf{w}_j | \Delta_{\mathcal{C}_{(j)}}^{\tilde{G}_S}(x_I, y_I, 1, 1) | \mathbf{w}_{j+1} - \mathbf{w}_j F B_0 - \mathbf{p}^I (L - I_k) B_0 \rangle$ . Let  $(\mathbf{w}_j : \mathbf{p}^I) \tilde{G}_S = (\mathbf{w}_j : \mathbf{p}^I : \mathbf{p}^P : \mathbf{w}_{j+1})$  where  $\tilde{G}_S$  is given in (14). Then

$$(\mathbf{w}_j : \mathbf{p}^I) \tilde{G} = \mathbf{w}_j : (\mathbf{p}^I L + \mathbf{w}_j F) : (\mathbf{w}_j C_0 + \mathbf{w}_j F E_0 + \mathbf{p}^I L E_0) : (\mathbf{w}_{j+1} + \mathbf{w}_j F B_0 + \mathbf{p}^I (L - I_k) B_0).$$

This implies

$$\langle \mathbf{w}_j | \Delta_{\mathcal{C}_{(j)}}^{\tilde{G}}(x_I, y_I, 1, 1) | \mathbf{w}_{j+1} + \mathbf{w}_j F B_0 + \mathbf{p}^I (L - I_k) B_0 \rangle = \langle \mathbf{w}_j | \Delta_{\mathcal{C}_{(j)}}^{\tilde{G}_S}(x_I, y_I, 1, 1) | \mathbf{w}_{j+1} \rangle,$$

and the result follows. ■

**Remark:** Although Theorem 17 seems very limited at a first glance, it applies to the families of rate  $1/n$  CCs without self-loops in the state diagram. This result does not hold for block codes; in this case,  $m = 0$  and the weight generating functions are not monomials.

In the following we present an example to illustrate Theorems 15 and 17. For convenience, we use the notation  $\Lambda_{\mathcal{C}_{(j)}}(y) = \Lambda_{\mathcal{C}_{(j)}}(x = 1, y)$ ,  $\Lambda_{\mathcal{C}_{(j)}}(y_I, y_P) = \Lambda_{\mathcal{C}_{(j)}}(x_I = 1, y_I, x_P = 1, y_P)$ , and  $\Delta_{\mathcal{C}_{(j)}}(y_I, y_O) = \Delta_{\mathcal{C}_{(j)}}(x_I = 1, y_P, x_O = 1, y_O)$ .

**Example 1.** Consider the constraint code of an  $(n = 2, k = 1, m = 2)$  CC over  $\mathbb{F}_2$  with the following generator matrices

$$\tilde{G}_S = \left( \begin{array}{c|cc|cc} 10 & 0 & 1 & 01 \\ 01 & 0 & 0 & 10 \\ 00 & 1 & 1 & 10 \end{array} \right) \text{ and } \tilde{G} = \left( \begin{array}{c|cc|cc} 10 & 0 & 1 & 01 \\ 01 & 1 & 1 & 00 \\ 00 & 1 & 1 & 10 \end{array} \right).$$

We have

$$\Lambda_{\mathcal{C}_{(j)}}^{\tilde{G}_S}(y_I, y_P) = \begin{pmatrix} 1 & y_I y_P & 0 & 0 \\ 0 & 0 & y_P & y_I \\ y_I y_P & 1 & 0 & 0 \\ 0 & 0 & y_I & y_P \end{pmatrix}$$

in the ordered basis  $\{|00\rangle, |10\rangle, |01\rangle, |11\rangle\}$ . By Theorem 17,

$$\Delta_{\tilde{\mathcal{C}}_{(j)}}^{\tilde{G}}(y_I, y_O) = \begin{pmatrix} 1 & y_I y_O^2 & 0 & 0 \\ 0 & 0 & y_O & y_I y_O \\ y_O^2 & y_I & 0 & 0 \\ 0 & 0 & y_O & y_I y_O \end{pmatrix}.$$

Note that

$$\Lambda_{\mathcal{C}_{(j)}}(y) = \begin{pmatrix} 1 & y^2 & 0 & 0 \\ 0 & 0 & y & y \\ y^2 & 1 & 0 & 0 \\ 0 & 0 & y & y \end{pmatrix}$$

is invariant as expected.

Also, from the MacWilliams identity for IOWAMs in Theorem 15, we have

$$\Lambda_{\tilde{\mathcal{C}}_{(j)}}^{\tilde{H}_S}(y_I, y_P) = \begin{pmatrix} 1 & 0 & y_I y_P & 0 \\ y_I y_P & 0 & 1 & 0 \\ 0 & y_P & 0 & y_I \\ 0 & y_I & 0 & y_P \end{pmatrix},$$

where  $\tilde{H}_S$  is the generator matrix of the constraint code of  $\mathcal{C}^\perp$ . □

#### D. Weight Enumeration for Convolutional Codes

In this subsection we will consider the Hamming weight enumeration on the codewords of a CC. Let  $\mathcal{C}$  be an  $(n, k, m)$  convolutional code over field  $\mathbb{F}_q$ . Recall that every codeword  $\mathbf{c} \in \mathcal{C}$  is of the following form

$$\mathbf{c} = \sum_{i=0}^d \mathbf{c}_i D^i$$

for some  $0 \leq d < \infty$ , with  $\mathbf{c}_i \in \mathcal{A}_n$  and  $\mathbf{c}_d \neq \mathbf{0}$ . We will say that the degree of  $\mathbf{c}$  is  $d$ , denoted by  $\deg(\mathbf{c}) = d$ . The Hamming weight of  $\mathbf{c} \in \mathcal{C}$  is given by a linear extension of the usual Hamming weight function to module  $\mathcal{M} = (\mathbb{F}_q[D])^n$ , i.e.,

$$\text{wt}(\mathbf{c}) = \sum_{i=0}^{\deg(\mathbf{c})} \text{wt}(\mathbf{c}_i).$$

**Definition 18.** The *total weight generating function*  $W_{\mathcal{C}}(y, D)$  of all codewords  $\mathbf{c} \in \mathcal{C}$  is given by the following in indeterminates  $y$  and  $D$ :

$$W_{\mathcal{C}}(y, D) = \sum_{\mathbf{c} \in \mathcal{C}} f_D(\mathbf{c}),$$

where

$$f_D(\mathbf{c}) := y^{\text{wt}(\mathbf{c})} D^{\deg(\mathbf{c})}$$

is a weight function of codewords  $\mathbf{c} \in \mathcal{C}$  in indeterminates  $y$  and  $D$ .

It is natural to consider the weight enumeration of a CC in one indeterminate since the codeword length is not fixed. Let  $\Lambda_{\mathcal{C}_{(j)}}(y) = \Lambda_{\mathcal{C}_{(j)}}(1, y)$  and (13) in Theorem 13 can be rewritten as

$$\Lambda_{\tilde{\mathcal{C}}_{(j)}}(y) = \frac{(1 + (q-1)y)^n}{q^{m+k}} \mathcal{F}_{\mathcal{A}_m} \Lambda_{\mathcal{C}_{(j)}} \left( \frac{1-y}{1+(q-1)y} \right) \mathcal{F}_{\mathcal{A}_m}^\dagger.$$

Without loss of generality, we assume the constraint codes  $\mathcal{C}_{(j)}$  of  $\mathcal{C}$  are the same for all  $j$ . Thus we have the following lemma that relates the total weight generating function  $W_{\mathcal{C}}(y, D)$  of a CC  $\mathcal{C}$  with its WAMs.

**Lemma 19.**

$$W_{\mathcal{C}}(y, D) = \langle 0 | (I_{q^m} - \Lambda_{\mathcal{C}_{(j)}}(y) D)^{-1} | 0 \rangle.$$

*Proof:* Note that any codeword  $\mathbf{c} \in \mathcal{C}$  with  $\deg(\mathbf{c}) = d$  must satisfy states  $\mathbf{w}_0 = \mathbf{0}$  and  $\mathbf{w}_j = \mathbf{0}$  for all  $j \geq d+1$ . Hence

$$\sum_{\substack{\mathbf{c} \in \mathcal{C} \\ \deg(\mathbf{c}) \leq d}} f_D(\mathbf{c}) = \langle 0 | \left( \sum_{i=0}^d (\Lambda_{\mathcal{C}_{(j)}}(y))^i D^i \right) | 0 \rangle.$$

Take  $d \rightarrow \infty$  and the result follows. ■

Applying Theorem 13 to the above lemma gives the following corollary.

**Corollary 20.**

$$W_{\mathcal{C}^\perp}(y, D) = \frac{1}{q^m} \langle 0 | \mathcal{F}_{\mathcal{A}_m} \left[ I_{q^m} - \frac{(1 + (q-1)y)^n}{q^k} \Lambda_{\mathcal{C}_{(j)}} \left( \frac{1-y}{1+(q-1)y} \right) D \right]^{-1} \mathcal{F}_{\mathcal{A}_m}^\dagger | 0 \rangle.$$

*Proof:* It follows from definition of  $W_{\mathcal{C}^\perp}(y, D)$  and Theorem 13 (taking  $x = 1$ ) that

$$\begin{aligned} W_{\mathcal{C}^\perp}(y, D) &= \langle 0 | \left( I_{q^m} - \Lambda_{\widehat{\mathcal{C}}_{(j)}}(y) D \right)^{-1} | 0 \rangle \\ &= \langle 0 | \left[ I_{q^m} - \frac{(1 + (q-1)y)^n}{q^{m+k}} \mathcal{F}_{\mathcal{A}_m} \Lambda_{\mathcal{C}_{(j)}} \left( \frac{1-y}{1+(q-1)y} \right) \mathcal{F}_{\mathcal{A}_m}^\dagger D \right]^{-1} | 0 \rangle \\ &= \frac{1}{q^m} \langle 0 | \mathcal{F}_{\mathcal{A}_m} \left[ I_{q^m} - \frac{(1 + (q-1)y)^n}{q^k} \Lambda_{\mathcal{C}_{(j)}} \left( \frac{1-y}{1+(q-1)y} \right) D \right]^{-1} \mathcal{F}_{\mathcal{A}_m}^\dagger | 0 \rangle. \end{aligned}$$

While Corollary 20 does not show the duality between  $W_{\mathcal{C}}(y, D)$  and  $W_{\mathcal{C}^\perp}(y, D)$ , we may reconsider enumerating walks on the full trellis diagram<sup>3</sup> of  $\mathcal{C}$  in a matrix, i.e.,

$$\Lambda_{\mathcal{C}}(y, D) := (I_{q^m} - \Lambda_{\mathcal{C}_{(j)}}(y) D)^{-1} = \sum_{d \geq 0} (\Lambda_{\mathcal{C}_{(j)}}(y))^d D^d,$$

whose  $(\mathbf{w}, \mathbf{w}')$  entry of the matrix  $(\Lambda_{\mathcal{C}_{(j)}}(y))^d$  is the enumeration of the Hamming weights of length- $d$  walks that begin at state  $\mathbf{w}$  at time 0 and end at state  $\mathbf{w}'$  at time  $d$  on the full trellis diagram of  $\mathcal{C}$ . Clearly, we have  $W_{\mathcal{C}}(y, D) = \langle 0 | \Lambda_{\mathcal{C}}(y, D) | 0 \rangle$ . It then follows from the proof of Corollary 20 that

$$\Lambda_{\mathcal{C}^\perp}(y, D) = \frac{1}{q^m} \mathcal{F}_{q^m} \Lambda_{\mathcal{C}} \left( \frac{1-y}{1+(q-1)y}, \frac{(1+(q-1)y)^n}{q^k} D \right) \mathcal{F}_{q^m}^\dagger \quad (17)$$

and  $W_{\mathcal{C}^\perp}(y, D) = \langle 0 | \Lambda_{\mathcal{C}^\perp}(y, D) | 0 \rangle$ .

Finally, we state the duality result for input-parity weight generating function for a systematic convolutional code  $\mathcal{C}$  in the following theorem.

**Theorem 21.** Suppose a CC  $\mathcal{C}$  is generated by a systematic encoder. For any codeword  $\mathbf{c} \in \mathcal{C}$ , let the weight function of  $\mathbf{c}$  be

$$f_D^{\text{IP}}(\mathbf{c}) = y_I^{\sum_{i=0}^{\deg(\mathbf{c})} \text{wt}(\mathbf{c}_{i,I})} y_P^{\sum_{i=0}^{\deg(\mathbf{c})} \text{wt}(\mathbf{c}_{i,P})} D^{\deg(\mathbf{c})},$$

where  $\mathbf{c}_i = (\mathbf{c}_{i,I} : \mathbf{c}_{i,P})$  is defined as before, and let  $W_{\mathcal{C}}(y_I, y_P, D)$  (resp.  $\Lambda_{\mathcal{C}}(y_I, y_P, D)$ ) be the input-parity weight generating function (resp. input-parity weight adjacency matrix) for codewords of  $\mathcal{C}$  (resp. walks on the full trellis diagram of  $\mathcal{C}$ ) defined with respect to the above weight function. Let  $\mathcal{C}^\perp$  be the dual code of  $\mathcal{C}$ ; then

$$\Lambda_{\mathcal{C}^\perp}(y_I, y_P, D) = \frac{1}{q^m} \mathcal{F}_{\mathcal{A}_m} \Lambda_{\mathcal{C}} \left( \frac{1-y_I}{1+(q-1)y_I}, \frac{1-y_P}{1+(q-1)y_P}, \frac{(1+(q-1)y_I)^k (1+(q-1)y_P)^{n-k}}{q^k} \right) \mathcal{F}_{\mathcal{A}_m}^\dagger.$$

Furthermore,

$$W_{\mathcal{C}}(y_I, y_P, D) = \langle 0 | \Lambda_{\mathcal{C}}(y_I, y_P, D) | 0 \rangle \quad \text{and} \quad W_{\mathcal{C}^\perp}(y_I, y_P, D) = \langle 0 | \Lambda_{\mathcal{C}^\perp}(y_I, y_P, D) | 0 \rangle.$$

#### E. Some Remarks on the Free-Distance Enumerator

Let  $\mathcal{C}$  be an  $(n, k, m)$  convolutional code.

**Definition 22.** The set  $\mathcal{C}_{\text{free}}$  consists of codewords  $\mathbf{c}$  whose state begins at  $\mathbf{w}_0 = 0$  and merges back into 0 at some smallest time instant  $d$ . More precisely,

$$\mathcal{C}_{\text{free}} = \left\{ \sum_{d \geq 0} \sum_{j=0}^d \mathbf{p}_j D^j : \begin{array}{l} (\mathbf{w}_j : \mathbf{p}_j : \mathbf{w}_{j+1}) \in \mathcal{C}_{(j)}, j = 0, \dots, d, \\ \mathbf{w}_0 = \mathbf{w}_{d+1} = 0, \mathbf{w}_j \neq 0 \text{ for } j = 1, \dots, d \end{array} \right\}.$$

Clearly, as an  $\mathbb{F}_q[D]$ -module, the code  $\mathcal{C}$  is generated by  $\mathcal{C}_{\text{free}}$  over  $\mathbb{F}_q[D]$ . But it should be noted that  $\mathcal{C}_{\text{free}}$  is not necessarily linear independent over  $\mathbb{F}_q[D]$ , nor a submodule of  $\mathcal{M}$ .

Following the notation in the previous section, we can enumerate the codewords in  $\mathcal{C}_{\text{free}}$  as

$$W_{\mathcal{C}_{\text{free}}}(y, D) = \sum_{\mathbf{c} \in \mathcal{C}_{\text{free}}} f_D(\mathbf{c}).$$

<sup>3</sup>By the full trellis diagram of  $\mathcal{C}$  we mean the trellis diagram of  $\mathcal{C}$  with arbitrary beginning and ending states.

The weight generating function  $W_{\mathcal{C}_{\text{free}}}(y, D)$  can be easily determined by the WAM of the constraint code  $\mathcal{C}_{(j)}$ .

**Proposition 23.** Let  $\Lambda_{\mathcal{C}_{(j)}}(y)$  be the weight adjacency matrix for the constraint code  $\mathcal{C}_{(j)}$ . Then

$$W_{\mathcal{C}_{\text{free}}}(y, D) = \langle 0 | [I_{q^m} - (\Lambda_{\mathcal{C}_{(j)}}(y) - |0\rangle\langle 0|) D]^{-1} | 0 \rangle \quad (18)$$

Remark: It should be noted that the above generating function differs from the conventional transfer function for convolutional codes in the sense that the zero element  $0 \in \mathcal{M}$  is excluded in the latter. The conventional transfer function of convolutional codes is given by  $W_{\mathcal{C}_{\text{free}}}(y, D) - f_D(0) = W_{\mathcal{C}_{\text{free}}}(y, D) - 1$ . Secondly, the minimal free-distance  $d_{\text{free}}$  of  $\mathcal{C}$  can be obtained by a power-series expansion of  $W_{\mathcal{C}_{\text{free}}}(y, D)$  in  $y$ , that is,

$$W_{\mathcal{C}_{\text{free}}}(y, D) = 1 + \sum_{i \geq d_{\text{free}}} \lambda_i y^i$$

for some rational function  $\lambda_i \in \mathbb{F}_q(D)$  with  $\lambda_{d_{\text{free}}} \neq 0$ .  $\square$

Note that the weight generating function for codewords  $\mathbf{c} \in \mathcal{C}$  is given by  $W_{\mathcal{C}}(y, D) = \langle 0 | (I_{q^m} - \Lambda_{\mathcal{C}_{(j)}}(y)D)^{-1} | 0 \rangle$ . Rewriting (18) as

$$W_{\mathcal{C}_{\text{free}}}(y, D) = \langle 0 | [(I_{q^m} - \Lambda_{(j)}(y)D) + |0\rangle\langle 0|D]^{-1} | 0 \rangle$$

and applying the Woodbury identity to the middle matrix, we can relate  $W_{\mathcal{C}_{\text{free}}}(y, D)$  to  $W_{\mathcal{C}}(y, D)$  as shown in the following corollary.

**Corollary 24.**

$$W_{\mathcal{C}_{\text{free}}}(y, D) = \frac{W_{\mathcal{C}}(y, D)}{1 + W_{\mathcal{C}}(y, D)D} \quad \text{and} \quad W_{\mathcal{C}}(y, D) = \frac{W_{\mathcal{C}_{\text{free}}}(y, D)}{1 - W_{\mathcal{C}_{\text{free}}}(y, D)D}.$$

*Proof:* By Woodbury identity for matrix inverse, we have

$$\begin{aligned} & [(I_{q^m} - \Lambda_{\mathcal{C}_{(j)}}(y)D) + |0\rangle\langle 0|D]^{-1} \\ &= (I_{q^m} - \Lambda_{\mathcal{C}_{(j)}}(y)D)^{-1} - \frac{D}{1 + \langle 0 | (I_{q^m} - \Lambda_{\mathcal{C}_{(j)}}(y)D)^{-1} | 0 \rangle D} (I_{q^m} - \Lambda_{\mathcal{C}_{(j)}}(y)D)^{-1} | 0 \rangle \langle 0 | (I_{q^m} - \Lambda_{\mathcal{C}_{(j)}}(y)D)^{-1}, \end{aligned}$$

which in turn gives

$$W_{\mathcal{C}_{\text{free}}}(y, D) = W_{\mathcal{C}}(y, D) - \frac{(W_{\mathcal{C}}(y, D))^2 D}{1 + W_{\mathcal{C}}(y, D)D} = \frac{W_{\mathcal{C}}(y, D)}{1 + W_{\mathcal{C}}(y, D)D}.$$

The second expression is then immediate.  $\blacksquare$

Remark: A much simpler way to prove Corollary 24 is to show the second expression directly. Note that  $\mathcal{C}$  is generated by  $\mathcal{C}_{\text{free}}$  over  $\mathbb{F}_q[D]$ , hence the result follows from the standard argument in enumerative combinatorics.

Let  $\mathcal{C}_{\text{free}}^{\perp}$  be the set consisting of the zero-path diverging codewords in  $\mathcal{C}^{\perp}$  and let  $W_{\mathcal{C}_{\text{free}}^{\perp}}(y, D) = \sum_{\mathbf{c} \in \mathcal{C}_{\text{free}}^{\perp}} f_D(\mathbf{c})$  be the corresponding weight generating function. Then by Corollary 24 we get

$$W_{\mathcal{C}_{\text{free}}^{\perp}}(y, D) = \frac{W_{\mathcal{C}^{\perp}}(y, D)}{1 + W_{\mathcal{C}^{\perp}}(y, D)D}.$$

One implication of the above is the following. There is a one-one correspondence, i.e. a duality, between  $\Lambda_{\mathcal{C}}(y, D)$  and  $\Lambda_{\mathcal{C}^{\perp}}(y, D)$  but not for  $W_{\mathcal{C}}(y, D)$  and  $W_{\mathcal{C}^{\perp}}(y, D)$ , since  $W_{\mathcal{C}}(y, D)$  corresponds only to the entry of  $\Lambda_{\mathcal{C}}(y, D)$  associated with  $(0, 0)$  as shown in Lemma 19. Thus, there is no one-one correspondence between  $W_{\mathcal{C}_{\text{free}}}(y, D)$  and  $W_{\mathcal{C}_{\text{free}}^{\perp}}(y, D)$  as observed by Shearer and McEliece more than 40 years ago [5]. On the other hand, let

$$\Lambda_{\mathcal{C}_{\text{free}}}(y, D) = [(I_{q^m} - \Lambda_{(j)}(y)D) + |0\rangle\langle 0|D]^{-1}$$

and

$$\Lambda_{\mathcal{C}_{\text{free}}^{\perp}}(y, D) = \left[ (I_{q^m} - \Lambda_{(j)^{\perp}}(y)D) + |0\rangle\langle 0|D \right]^{-1}$$

denote the enumerations of length- $d$  walks from state  $\mathbf{w}$  to  $\mathbf{w}'$  without immediate loops at state 0 in the full trellis diagrams of  $\mathcal{C}$  and  $\mathcal{C}^{\perp}$ , respectively. Clearly,

$$W_{\mathcal{C}_{\text{free}}}(y, D) = \langle 0 | \Lambda_{\mathcal{C}_{\text{free}}}(y, D) | 0 \rangle \quad \text{and} \quad W_{\mathcal{C}_{\text{free}}^{\perp}}(y, D) = \langle 0 | \Lambda_{\mathcal{C}_{\text{free}}^{\perp}}(y, D) | 0 \rangle.$$

Most importantly, there is indeed a one-one correspondence between  $\Lambda_{\mathcal{C}_{\text{free}}}(y, D)$  and  $\Lambda_{\mathcal{C}_{\text{free}}^{\perp}}(y, D)$  implied by (17). We summarize the above relations in a diagram as shown in Fig. 3.

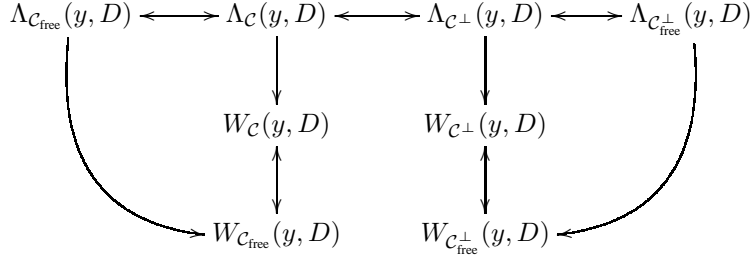


Fig. 3. Relations diagram of various weight enumerations. A relation  $A \rightarrow B$  means that  $B$  can be derived given  $A$ .

#### IV. THE MACWILLIAMS IDENTITY FOR QUANTUM CONVOLUTIONAL CODES

In this section we develop the duality theorem for EA-QCC. We begin with an introduction to the theory of EAQECCs and QCCs in the next two subsections, followed by the duality theorem and the MacWilliams identity for EA-QCCs. The readers can safely skip the next two subsections if they are familiar with quantum coding theory.

##### A. Quantum Error-Correcting Codes

Let us introduce some basic notions of quantum mechanics. In this section, we denote  $\mathcal{H}$  the state space of a single qubit with an (ordered) orthonormal computation basis  $\{|0\rangle, |1\rangle\}$ . The state space of  $n$  qubits is the tensor product of  $n$  single qubit state space  $\mathcal{H}$  and is denoted by  $\mathcal{H} \otimes \cdots \otimes \mathcal{H} = \mathcal{H}^{\otimes n}$ . Let  $\mathcal{G}_n = \mathcal{G}_1^{\otimes n}$  denote the  $n$ -fold Pauli group, where  $\mathcal{G}_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$ . Note that  $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ ,  $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ ,  $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ , and  $Y = iZX$  form a basis of the space of the linear operators on  $\mathcal{H}$ . The weight  $\text{wt}(g)$  of  $g \in \mathcal{G}_n$  is the number of components of  $g$  that are not the identity operator. Let  $Z_i = I^{\otimes i-1} Z I^{\otimes n-i}$  and  $X_i = I^{\otimes i-1} X I^{\otimes n-i}$  be the Pauli operators on the  $i$ -th qubit for convenience and the total number of qubits is clear from the context. For  $g, h \in \mathcal{G}_n$ , we define the symplectic inner product  $*$  in  $\mathcal{G}_n$  by

$$g * h = \begin{cases} 0, & \text{if } gh - hg = 0; \\ 1, & \text{if } gh + hg = 0. \end{cases}$$

We first define the *seed transformation* on the  $n$ -fold Pauli group  $\mathcal{G}_n$ , which is a unitary Clifford operator that preserves  $\mathcal{G}_n$  under conjugation [38], [18], [21].

**Definition 25.** A seed transformation  $U$  on  $\mathcal{H}^{\otimes n}$  is a unitary Clifford operator so that  $UZ_i U^\dagger = g_i \in \mathcal{G}_n$ ,  $UX_i U^\dagger = h_i \in \mathcal{G}_n$ , for  $i = 1, \dots, n$ .

Thus  $\{g_1, \dots, g_n, h_1, \dots, h_n\}$  forms a set of  $n$  pairs of symplectic partners, satisfying the commutation relation

$$\begin{aligned} g_i * h_i &= 1, \\ g_i * h_j &= 0, \\ g_i * g_j &= 0, \\ h_i * h_j &= 0, \end{aligned} \tag{19}$$

for  $i \neq j$ .

Suppose  $\mathcal{S}$  is an Abelian subgroup of  $\mathcal{G}_n$  with a set of  $n - k$  independent generators defined by a seed transformation  $U$  as

$$\mathcal{S} = \{U(I^{\otimes k} \otimes S^Z)U^\dagger : S^Z \in \{I, Z\}^{\otimes n-k}\}$$

and  $\mathcal{S}$  does not include  $-I$ . An  $[[n, k]]$  quantum stabilizer code  $C(\mathcal{S})$  is defined as the  $2^k$ -dimensional subspace of  $\mathcal{H}^{\otimes n}$  fixed by  $\mathcal{S}$ . That is,

$$C(\mathcal{S}) = \{|\psi\rangle \in \mathcal{H}^{\otimes n} : g|\psi\rangle = |\psi\rangle, \forall g \in \mathcal{S}\}.$$

The seed transformation  $U$  is an encoding operator of  $C(\mathcal{S})$ . In this definition we implicitly assume that the first  $k$  qubits before encoding are logical qubits and the last  $n - k$  ancilla states begin in  $|0\rangle$ . The normalizer group  $N(\mathcal{S})$  of  $\mathcal{S}$  is the set of logical operators in  $\mathcal{G}_n$  that commute with the stabilizers and do not affect the outcomes when the stabilizers are measured. It is given by

$$\begin{aligned} N(\mathcal{S}) &= \{f \in \mathcal{G}_n : fgf^\dagger \in \mathcal{S}, \forall g \in \mathcal{S}\} \\ &= \{U(L \otimes S^Z)U^\dagger : S^Z \in \{I, Z\}^{\otimes n-k}, L \in \mathcal{G}_k\}. \end{aligned}$$

Note that the orthogonal group of  $\mathcal{S}$  with respect to  $*$  is  $\mathcal{S}^\perp = \{h \in \mathcal{G}_n : h * g = 0, \forall g \in \mathcal{S}\} = N(\mathcal{S})$ .

If the sender and receiver share  $c$  maximally-entangled pairs  $|\Phi_+\rangle^{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$  before communication, this coding scheme is called an entanglement-assisted quantum error-correcting code (EAQECC) [20], [21]. Similarly, an  $[[n, k; c]]$

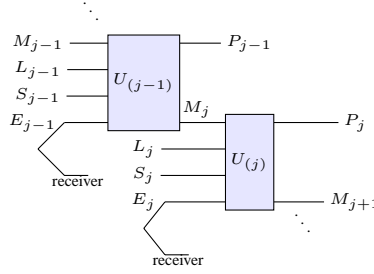


Fig. 4. Circuit diagram of an EA-QCC encoder with a seed transformation  $U$ .

EAQECC is defined to be the  $2^k$ -dimensional subspace of  $\mathcal{H}^{\otimes n} \otimes \mathcal{H}^{\otimes c}$  fixed by a stabilizer group  $\mathcal{S} \in \mathcal{G}_{n+c}$ . It is assumed that the qubits held by the receiver before communication are error-free and thus we neglect the operators on the halves of the maximally-entangled pairs of the receiver. (The case that the qubits of the receiver are imperfect is addressed in [39]). Again we assume that the first  $k$  qubits before encoding are information qubits, the last  $c$  qubits are halves of the maximally-entangled states, and the other ancilla states begin in  $|0\rangle$ .<sup>4</sup> Suppose  $\mathcal{S}'$  is defined by a seed transformation  $U$  on  $n$  qubits by

$$\mathcal{S}' = \{U(I^{\otimes k} \otimes S^Z \otimes S^E)U^\dagger : S^Z \in \{I, Z\}^{\otimes n-k-c}, S^E \in \{I, X, Y, Z\}^{\otimes c}\}.$$

In this case the simplified stabilizer group  $\mathcal{S}'$  is no longer Abelian. Now the set of all possible logical operators  $N(\mathcal{S}')$  is

$$N(\mathcal{S}') = \{U(L \otimes S^Z \otimes I^{\otimes c})U^\dagger : S^Z \in \{I, Z\}^{\otimes n-k-c}, L \in \mathcal{G}_k\}.$$

### B. Quantum Convolutional Codes

Like a classical CC, an EA-QCC encodes a stream of operators as shown in Fig. 4. We will define an EA-QCC by a seed transformation unitary similarly to the development in Section III-B. Again, it is assumed that the halves of the maximally-entangled states held by the receiver are perfect and the operators on these qubits are ignored.

An  $((n, k, c, m))$  EA-QCC  $\mathcal{C}$  has an  $m$ -qubit memory state and it outputs an  $n$ -qubit encoded state from a  $k$ -qubit logical state at each time step. Suppose  $\mathcal{C}$  is defined by the seed transformations  $U_{(j)}$  on  $\mathcal{H}^{\otimes(n+m)}$  with input parameters  $(\mathcal{I}^M, \mathcal{I}^L, \mathcal{I}^A, \mathcal{I}^E)$ , and output parameters  $(\mathcal{I}^{M'}, \mathcal{I}^P)$ , where  $\mathcal{I}^M, \mathcal{I}^L, \mathcal{I}^A, \mathcal{I}^E, \mathcal{I}^{M'}$ , and  $\mathcal{I}^P \subset \{1, 2, \dots, n+m\}$  are the locations of the input memory qubits, logical qubits, ancilla qubits, entangled qubits, output memory qubits, and physical qubits, so that  $|\mathcal{I}^M| = |\mathcal{I}^{M'}| = m$ ,  $|\mathcal{I}^L| = k$ ,  $|\mathcal{I}^A| = a$ ,  $|\mathcal{I}^E| = c$ , and  $|\mathcal{I}^P| = n = k + a + c$ . Let  $M_j, M_{j+1} \in \{I, X, Y, Z\}^{\otimes m}$  be the memory operators at time steps  $j$  and  $j+1$ , respectively, and let  $\{L_j \in \mathcal{G}_k\}$  be the stream of logical operators. The seed transformation  $U_{(j)}$  works like an EAQECC encoding operator and it produces a truncated<sup>5</sup> stabilizer group  $\bar{\mathcal{S}}_{(j)}$  and a logical set  $N(\bar{\mathcal{S}}_{(j)})$  based on  $M_j$  at each time step  $j$ . Consequently, the EA-QCC  $\mathcal{C}$  is the state space stabilized by the stabilizer group  $\bigotimes_j \bar{\mathcal{S}}_{(j)}$ , where  $\bigotimes_j \bar{\mathcal{S}}_{(j)} = \{\bigotimes_j g_{(j)} : g_{(j)} \in \bar{\mathcal{S}}_{(j)}\}$ . For convenience, we assume a seed transformation operates on input memory qubits, logical qubits, ancilla qubits, and entangled qubits in order, and its output are memory qubits and physical qubits in order, unless otherwise specified. More precisely, we have

$$\begin{aligned} \bar{\mathcal{S}}_{(j)} = \{ & P_j \in \{I, X, Y, Z\}^{\otimes n} : P_j \otimes M_{j+1} = U(M_j \otimes I^{\otimes k} \otimes S_j \\ & \otimes E_j)U^\dagger \text{ for } M_j \in \{I, X, Y, Z\}^{\otimes m}, S_j \in \{I, Z\}^{\otimes n-k-c}, \\ & E_j \in \{I, X, Y, Z\}^{\otimes c} \} \end{aligned}$$

and

$$\begin{aligned} N(\bar{\mathcal{S}}_{(j)}) = \{ & P_j \in \mathcal{G}_n : P_j \otimes M_{j+1} = U(M_j \otimes L_j \otimes S_j \otimes I^{\otimes c})U^\dagger \\ & \text{for } M_j \in \{I, X, Y, Z\}^{\otimes m}, S_j \in \{I, Z\}^{\otimes n-k-c}, L_j \in \mathcal{G}_k \}. \end{aligned}$$

Note that an  $((n, k, m))$  QCC is a special case of  $c = 0$ .

Below we give a definition of the dual of an EA-QCC.

**Definition 26.** Suppose  $\mathcal{C}$  is an EA-QCC defined by the seed transformations  $U_{(j)}$  on  $\mathcal{H}^{\otimes(n+m)}$  with input parameters  $(\mathcal{I}^M, \mathcal{I}^L, \mathcal{I}^A, \mathcal{I}^E)$ . Then the dual code  $\mathcal{C}^\perp$  of  $\mathcal{C}$  is defined by the seed transformations  $U_{(j)}$  with input parameters  $(\mathcal{I}^M, \mathcal{I}^E, \mathcal{I}^A, \mathcal{I}^L)$ . The output parameters  $(\mathcal{I}^{M'}, \mathcal{I}^P)$  are the same for  $\mathcal{C}$  and  $\mathcal{C}^\perp$ .

<sup>4</sup>Notice that the order of these qubits is important since it affects the definition of the dual code. Our definition can be generalized by specifying the locations of the the maximally-entangled qubits, the ancilla qubits, and the information qubits, respectively as in [17].

<sup>5</sup>Note that the part of operators on memory qubits are discarded in this truncated stabilizer group, which is slightly different in the definition of the simplified stabilizer group of an EAQECC.

Consider the normal factor graph (Fig. 2) of an EA-QCC  $\mathcal{C}$ . Its constraint code  $\mathcal{C}_{(j)}$  at time  $j$  is the  $[[n+2m, k; c]]$  EAQECC defined by a simplified stabilizer group  $\mathcal{S}_{(j)}$  with the following generators:

$$\begin{aligned} Z_i^M \otimes g_i, X_i^M \otimes h_i, & \quad \text{for } i \in \mathcal{I}^M; \\ I^M \otimes g_i, I^M \otimes h_i, & \quad \text{for } i \in \mathcal{I}^E; \\ I^M \otimes g_i, & \quad \text{for } i \in \mathcal{I}^A, \end{aligned}$$

where  $Z_i^M, X_i^M, I^M \in \mathcal{G}_m$  and  $g_i = U_{(j)} Z_i U_{(j)}^\dagger$ ,  $h_i = U_{(j)} X_i U_{(j)}^\dagger \in \mathcal{G}_{n+m}$ . According to [17], the dual code  $\mathcal{C}_{(j)}^\perp$  with respect to the inner product  $*$ , defined in  $\mathcal{G}_{n+2m}$ , is the  $[[n+2m, c; k]]$  EAQECC defined by a simplified stabilizer group  $\mathcal{S}_{(j)}^\perp$  with the following generators:

$$\begin{aligned} Z_i^M \otimes g_i, X_i^M \otimes h_i, & \quad \text{for } i \in \mathcal{I}^M; \\ I^M \otimes g_i, I^M \otimes h_i, & \quad \text{for } i \in \mathcal{I}^L; \\ I^M \otimes g_i, & \quad \text{for } i \in \mathcal{I}^A. \end{aligned}$$

Observe that the seed transformation  $U_{(j)}$  with the input parameters  $(\mathcal{I}^M, \mathcal{I}^E, \mathcal{I}^A, \mathcal{I}^L)$  as in Definition 26 defines the dual constraint code  $\mathcal{C}_{(j)}^\perp$ . Following [13], this constraint code  $\mathcal{C}_{(j)}^\perp$  defines the dual graph of the normal factor graph of the original quantum convolutional code. Thus our definition of the dual code of a quantum convolutional code is justified.

An EA-QCC and its dual are uniquely defined up to a *unitary row operator*  $R$  that preserves  $\mathcal{S}_{(j)}$  and  $\mathcal{S}_{(j)}^\perp$  [40]. For example,  $U_{(j)} R$  is a seed transformation that defines the same EA-QCC as  $U_{(j)}$  does if for all  $g \in \mathcal{S}_{(j)}$  and  $h \in \mathcal{S}_{(j)}^\perp$ ,  $RgR^\dagger \in \mathcal{S}_{(j)}$  and  $RhR^\dagger \in \mathcal{S}_{(j)}^\perp$ , respectively.

**Remark:** One can define a polynomial check matrix  $S(D)$  as in [23], [24] and show that  $S(D)$  can be obtained from the seed transformation  $U$  by finding an equation like the classical case in (7). Then we can use this equation to verify the orthogonality between an EA-QCC and its dual with respect to the symplectic inner product  $*$ . However, the orthogonality is obvious since the EA-QCC is encoded by

$$\prod_j D^{j-1} [U_{(j)}],$$

where  $D[A] = I^{\otimes n} \otimes A$  is a delay operation on an operator  $A$  so that the operation of  $A$  is shifted by  $n$  qubits. We postpone the introduction of the polynomial check matrix  $S(D)$  to Appendix B.

### C. The MacWilliams Identity for EA-QCCs

Now we proceed to derive the MacWilliams identity for EA-QCCs.

Since the overall phase of a quantum state is not important, it is sufficient to consider Pauli operators in the quotient group  $\bar{\mathcal{G}}_n = \mathcal{G}_n / \{\pm 1, \pm i\}$ . An element in  $\bar{\mathcal{G}}_n$  is denoted by  $[g]$ , where  $g \in \mathcal{G}_n$ . Thus  $[\ ]$  defines an equivalence class. If  $[g] = [g']$  in  $\bar{\mathcal{G}}_n$ , then  $gg' \in \{\pm 1, \pm i\}$ . For  $[g_1], [g_2] \in \bar{\mathcal{G}}_n$ , we define the symplectic inner product  $*$  by  $[g_1] * [g_2] = g_1 * g_2$ .

The weight generating function of a set  $\mathcal{S} \subset \mathcal{G}_n$  is  $g_{\mathcal{S}}(x, y) = \sum_{w=0}^n \nu_w x^{n-w} y^w$ , where  $\nu_w$  is the number of elements of  $[\mathcal{S}] = \mathcal{S} / \{\pm 1, \pm i\}$  of weight  $w$ . The WAMs of EA-QCCs are defined similarly to the classical case as follows.

**Definition 27.** The WAM  $\Lambda_{\mathcal{C}_{(j)}}(x, y)$  of an EA-QCC  $\mathcal{C}$  with constraint codes  $\mathcal{C}_{(j)}$  defined by simplified stabilizer groups  $\mathcal{S}_{(j)}$  is the matrix whose  $(M_j, M_{j+1})$  entry is the weight generating function of the set of physical output operators  $\{P_j \in \mathcal{S}_{(j)}\}$  when the input and output memory operators are  $M_j$  and  $M_{j+1}$ , respectively.

In the case of the quotient Pauli group  $\bar{\mathcal{G}}_1 = \langle [I], [X], [Y], [Z] \rangle$  (in order), which is isomorphic to  $\mathbb{Z}_2^2$ , the matrix representation of the Fourier transform operator  $\mathcal{F}_{\bar{\mathcal{G}}_1} \equiv F$  in the ordered basis  $|[I]\rangle, |[X]\rangle, |[Y]\rangle, |[Z]\rangle$  is

$$F = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}. \quad (20)$$

It can be verified that the Fourier transform matrix on the  $n$ -fold Pauli group  $\bar{\mathcal{G}}_n$  is  $F^{\otimes n}$  as in Lemma 2.

The MacWilliams identity for EA-QCCs is a straightforward application of Theorem 13, and the proof is omitted.

**Theorem 28.** Suppose the WAM of an  $((n, k, c, m))$  EA-QCC  $\mathcal{C}$  is  $\Lambda_{\mathcal{C}_{(j)}}(x, y)$ . Then the WAM of its dual  $\mathcal{C}^\perp$  is

$$\Lambda_{\mathcal{C}_{(j)}^\perp}(x, y) = 4^{-m} 4^{-k} 2^{-a} F^{\otimes m} \Lambda_{\mathcal{C}_{(j)}}(x + 3y, x - y) F^{\otimes m},$$

where  $F$  is the Fourier transform matrix defined in (20). Let  $\Lambda_{\mathcal{C}_{(j)}}(y) = \Lambda_{\mathcal{C}_{(j)}}(1, y)$ , and the MacWilliam identity can be



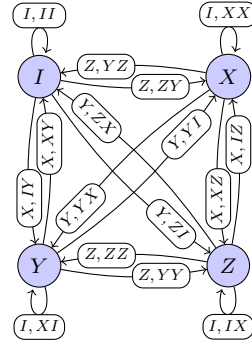


Fig. 5. The state diagram corresponding to the seed transformation  $U_1$  given in (21).

rewritten as

$$\Lambda_{C_{(j)}}^{\perp}(y) = \frac{(1+3y)^n}{4^m 4^k 2^a} F^{\otimes m} \Lambda_{C_{(j)}} \left( \frac{1-y}{1+3y} \right) F^{\otimes m}.$$

In the case of  $m = 0$ , it reduces to the case of EAQECs in [41], [17].

In the following we provide some examples.

**Example 2.** Wilde and Hsieh constructed an example of non-catastrophic and recursive ( $(n = 2, k = 1, c = 1, m = 1)$ ) EA-QCC with  $\mathcal{I}^M = \{1\}$ ,  $\mathcal{I}^{L'} = \{2\}$ ,  $\mathcal{I}^E = \{3\}$ ,  $\mathcal{I}^{M'} = \{1\}$ ,  $\mathcal{I}^P = \{2, 3\}$ , and the following seed transformation  $U_1$  [28]:

$$\begin{array}{ccc|ccc} Z & I & I & Z & I & X \\ I & Z & I & X & Z & Y \\ I & I & Z & X & Y & Z \\ X & I & I & X & X & X \\ I & X & I & Y & I & Y \\ I & I & X & Y & X & Y \end{array} \xrightarrow{U_1} \quad (21)$$

Its state diagram is shown in Fig. 5.

The WAM<sup>6</sup> of this EA-QCC can be computed easily:

$$\Lambda_{C_{(j)}}(y) = \begin{bmatrix} 1 & y^2 & y & y \\ y^2 & y^2 & y^2 & y^2 \\ y^2 & y & y & y^2 \\ y^2 & y & y^2 & y \end{bmatrix}.$$

The dual of this EA-QCC is obtained by switching the roles of the logical qubits and ebits, and in this example  $k = c = 1$ . We found the state diagram of the dual code is the reversed graph of the original state diagram, and consequently it has a weight adjacency matrix  $\Lambda_{C_{(j)}}^{\perp}(W) = \Lambda_{C_{(j)}}^{\top}(W)$ .

On the other hand, we can apply Theorem 28 to obtain the same result as well.  $\square$

The MacWilliams identity holds for the EA-QCCs, catastrophic or noncatastrophic, recursive or nonrecursive (see Refs [27], [29] for these definitions).

**Example 3.** Consider the seed transformation of an ( $(n = 2, k = 1, c = 1, m = 1)$ ) catastrophic and non-recursive EA-QCC  $U_2$  is as follows:

$$\begin{array}{ccc|ccc} Z & I & I & Z & I & I \\ I & Z & I & Z & Z & I \\ I & I & Z & I & Z & Z \\ X & I & I & X & X & X \\ I & X & I & I & X & X \\ I & I & X & I & I & X \end{array} \xrightarrow{U_2} \quad (22)$$

<sup>6</sup>The definition of WAM in [28] removes the path of the zero physical-weight cycle at the (0,0) entry in order to compute the free distance. Therefore, our definition is more general.

( $\mathcal{I}^M = \{1\}$ ,  $\mathcal{I}^{L'} = \{2\}$ ,  $\mathcal{I}^E = \{3\}$ ,  $\mathcal{I}^{M'} = \{1\}$ , and  $\mathcal{I}^P = \{2, 3\}$ .) The WAMs of this EA-QCC and its dual are

$$\Lambda_{C_{(j)}}(y) = \begin{bmatrix} 1+y^2 & 0 & 0 & y+y^2 \\ 0 & 1+y^2 & y+y^2 & 0 \\ 0 & y+y^2 & 1+y^2 & 0 \\ y+y^2 & 0 & 0 & 1+y^2 \end{bmatrix},$$

and

$$\Lambda_{C_{(j)}^\perp}(y) = \begin{bmatrix} 1+y+2y^2 & 0 & 0 & 0 \\ 0 & y+3y^2 & 0 & 0 \\ 0 & 0 & y+3y^2 & 0 \\ 0 & 0 & 0 & 1+y+2y^2 \end{bmatrix}.$$

□

In the following example, we will demonstrate that sometimes it is easier to compute the WAM of a QCC by first computing the WAM of its dual code and applying Theorem 28.

**Example 4.** Consider the  $((n = 2, k = 1, m = 1))$  QCC constructed in [27] with the same seed transformation  $U_2$ , but  $\mathcal{I}^{M'} = \{3\}$  and  $\mathcal{I}^P = \{1, 2\}$ . The dual code of this QCC is the  $((n = 2, k = 0, c = 1, m = 1))$  EA-QCC. The state diagram of this EA-QCC can be easily constructed by removing those edges of the original state diagram with nonzero logical weight. Therefore, the WAM of the dual code is

$$\Lambda_{C_{(j)}^\perp}(y) = \begin{bmatrix} 1 & 0 & 0 & y \\ 0 & y^2 & y^2 & 0 \\ 0 & y^2 & y^2 & 0 \\ y & 0 & 0 & y^2 \end{bmatrix}.$$

The WAM of the original QCC can be obtained by Theorem 28 as follows:

$$\begin{aligned} \Lambda_{C_{(j)}}(y) &= \frac{(1+3y)^n}{4^m 4^c 2^a} F^{\otimes m} \Lambda_{C_{(j)}^\perp} \left( \frac{1-y}{1+3y} \right) F^{\otimes m} \\ &= \begin{bmatrix} 1+y^2 & y+y^2 & y+y^2 & 2y \\ y+y^2 & 2y^2 & 2y^2 & y+y^2 \\ y+y^2 & 2y^2 & 2y^2 & y+y^2 \\ 2y & y+y^2 & y+y^2 & 1+y^2 \end{bmatrix}. \end{aligned}$$

□

## V. CONCLUSION

In this paper, we detailed various notions of weight enumeration of convolutional codes and summarized their relations in Fig. 3. The MacWilliams theorem for convolutional codes is thus completed. With a different representation of the EWGF in our paper, we provided a direct proof of the MacWilliams identity for the convolutional codes. This method allows us to develop the MacWilliams identity for the IOWAMs of a CC and its dual with systematic encoders, which answers an open question in [11]. The input-output weight distributions are an essential part in the error analysis of iterative decoding, in particular for turbo codes. Our result could potentially lead to preliminary error analysis of both classical and quantum turbo codes.

Although we did not discuss the complete weight generating functions of linear block codes or the complete weight adjacency matrices of CCs, these functions can be similarly defined and the MacWilliams identities for these functions follow as a corollary of Theorem 3 as well. It is also straightforward to generalize the MacWilliams identity for IOWAMs for terminated convolutional codes [13], [42] and derive the quantum analogues.

Another contribution of this work is a MacWilliams identity for the EA-QCCs. Specifically, the MacWilliams identity is established for the WAMs of an EA-QCC and its dual. Our definition of the dual code of an EA-QCC is similar to that of an EAQECC. Although it is also easy to construct the MacWilliams identity for split weight enumeration, the meaning of split weight enumeration is not clear.

The free distance of a CC is an important parameter to characterize its error performance. An upper bound on the free distance is the Plotkin-type bound [8]. This upper bound can be directly applied to a CC or its dual. It is desired to obtain a similar bound for the quantum case; however, the quantum Plotkin bound is not tight [41]. It seems that the free distance of an EA-QCC is closely related to the minimum distance of its constraint code. On the other hand, the MacWilliams identity leads to the linear programming bounds for block codes. It is not obvious if we can derive a similar upper bound for CCs.

Unlike classical codes, QECCs can involve various different resources [43], [44]. Another interesting open question is how to quantify the *passive* error-correcting power of the quantum subsystem codes; particularly, using the weight generating functions or weight generating functions. It is possible to define the dual codes of such QECCs and obtain various notions of

MacWilliams identities. However, it remains unknown that these quantum weight generating functions can be directly applied to the performance analysis for these codes. The main difficulty arises from the quantum effect; namely, quantum degeneracy.

#### ACKNOWLEDGMENT

CYL was supported by the Australian Research Council under Grant DP120103776. MH was supported by the UTS Chancellors postdoctoral research fellowship and UTS Early Career Researcher Grants Scheme.

#### APPENDIX A WEIGHT ENUMERATION OF THE CONSTRAINT CODE

Let  $\mathcal{V}$  be a vector space over  $\mathbb{F}_q$  and assume  $\mathbb{F}_q$  has characteristic  $p$ . The group character  $\chi_{\mathbf{u}} \in \text{Hom}(\mathcal{V}, U(1))$  for some  $\mathbf{u} \in \mathcal{V}$  is a group homomorphism from  $\mathcal{V}$  to  $U(1)$ , the unitary group in  $\mathbb{C}$ . Below we will focus on a specific kind of group character  $\chi_{\mathbf{u}} : \mathbf{v} \mapsto \omega^{\text{tr}(\mathbf{u}^T \mathbf{v})}$ , where  $\text{tr} : \mathbb{F}_q \rightarrow \mathbb{F}_p$  is the usual trace linear map for fields, and  $\omega$  is a primitive  $p$ -th root of unity in  $\mathbb{C}$ . Note that in this appendix,  $\mathbf{v}$  is considered as a column vector.

Let  $\mathcal{V} = \mathbb{F}_q^{2m+n}$  and  $f$  be any function defined on  $\mathcal{V}$ . The classical MacWilliams identity is simply

$$\sum_{\mathbf{v} \in \mathcal{C}_{(j)}^\perp} f(\mathbf{v}) = \frac{1}{|\mathcal{C}_{(j)}|} \sum_{\mathbf{u} \in \mathcal{C}_{(j)}} F(\mathbf{u}) \quad (22)$$

where  $F$  is the Fourier transform of  $f$  over  $\mathcal{V}$  with respect to kernel  $\chi_{\mathbf{u}}(\mathbf{v})$ .

##### A. Enumerate in Multivariate Polynomial

For any  $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) \in \mathbb{F}_q^m \times \mathbb{F}_q^n \times \mathbb{F}_q^m \cong \mathcal{V}$ , in this subsection we consider the following weight function

$$f(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) = \left[ \prod_{i=1}^m \prod_{j=1}^q x_{i,j}^{\text{wt}_j(v_{1,i})} \right] y^{\text{wt}(\mathbf{v}_2)} \left[ \prod_{i=1}^m \prod_{j=1}^q z_{i,j}^{\text{wt}_j(v_{3,i})} \right]$$

for some indeterminates  $x_{i,j}$ ,  $y$ , and  $z_{i,j}$ , where  $\mathbf{v}_1, \mathbf{v}_3 \in \mathbb{F}_q^m$ ,  $\mathbf{v}_2 \in \mathbb{F}_q^n$ , and  $\text{wt} : \mathbb{F}_q^n \rightarrow \mathbb{Z}^+$  is the usual Hamming weight metric. Say  $\mathbb{F}_q = \{\alpha_1, \dots, \alpha_q\}$ ,  $\text{wt}_j$  is an indicator function given by  $\text{wt}_j(a) := 1(a = \alpha_j)$ .

The weight enumerator for  $\mathcal{C}_{(j)}$  based on weight function  $f$  is

$$W_{\mathcal{C}_{(j)}}(x_{1,1}, \dots, x_{m,q}, y, z_{1,1}, \dots, z_{m,q}) = \sum_{(\mathbf{w}_j^T : \mathbf{p}_j^T : \mathbf{w}_{j+1}^T)^T \in \mathcal{C}_{(j)}} f(\mathbf{w}_j, \mathbf{p}_j, \mathbf{w}_{j+1}).$$

The Fourier transform of  $f$  over  $\mathcal{V}$  with respect to kernel  $\chi_{\mathbf{u}}(\mathbf{v})$  with  $\mathbf{u} = (\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$  is given by

$$\begin{aligned} & F(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3) \\ &= \sum_{(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) \in \mathcal{V}} f(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) [\chi_{\mathbf{u}}(\mathbf{v})]^* \\ &= \sum_{(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) \in \mathcal{V}} \left[ \prod_{i=1}^m \prod_{j=1}^q x_{i,j}^{\text{wt}_j(\mathbf{v}_1)} \right] y^{\text{wt}(\mathbf{v}_2)} \left[ \prod_{i=1}^m \prod_{j=1}^q z_{i,j}^{\text{wt}_j(\mathbf{v}_3)} \right] \omega^{-\sum_{i=1}^3 \text{tr}(\mathbf{u}_i^T \mathbf{v}_i)} \\ &= \left[ \prod_{i=1}^m \left( \sum_{v \in \mathbb{F}_q} \omega^{-\text{tr}(u_{1,i} v)} \prod_{j=1}^q x_{i,j}^{\text{wt}_j(v)} \right) \right] \left[ \prod_{i=1}^n \left( \sum_{v \in \mathbb{F}_q} y^{\text{wt}(v)} \omega^{-\text{tr}(u_{2,i} v)} \right) \right] \left[ \prod_{i=1}^m \left( \sum_{v \in \mathbb{F}_q} \omega^{-\text{tr}(u_{3,i} v)} \prod_{j=1}^q z_{i,j}^{\text{wt}_j(v)} \right) \right] \\ &= \left[ \prod_{i=1}^m \left( \sum_{j=1}^q \omega^{-\text{tr}(u_{1,i} \alpha_j)} x_{i,j} \right) \right] (1 + (q-1)y)^{n-\text{wt}(\mathbf{u}_2)} (1-y)^{\text{wt}(\mathbf{u}_2)} \left[ \prod_{i=1}^m \left( \sum_{j=1}^q \omega^{-\text{tr}(u_{3,i} \alpha_j)} z_{i,j} \right) \right] \\ &= \left[ \prod_{i=1}^m \prod_{\ell=1}^q \left( \sum_{j=1}^q \omega^{-\text{tr}(\alpha_\ell \alpha_j)} x_{i,j} \right) \right]^{\text{wt}_\ell(u_{1,i})} (1 + (q-1)y)^{n-\text{wt}(\mathbf{u}_2)} (1-y)^{\text{wt}(\mathbf{u}_2)} \left[ \prod_{i=1}^m \prod_{\ell=1}^q \left( \sum_{j=1}^q \omega^{-\text{tr}(\alpha_\ell \alpha_j)} z_{i,j} \right) \right]^{\text{wt}_\ell(u_{3,i})}. \end{aligned}$$

Thus we obtain the following theorem.

**Theorem 29.** The weight enumerators for  $\mathcal{C}_{(j)}^\perp$  and  $\widehat{\mathcal{C}}_{(j)}$  are given by

$$\begin{aligned}
W_{\mathcal{C}_{(j)}^\perp}(x_{1,1}, \dots, x_{m,q}, y, z_{1,1}, \dots, z_{m,q}) &= \frac{(1 + (q-1)y)^n}{q^{m+k}} W_{\mathcal{C}_{(j)}}(x_{1,1}, \dots, x_{m,q}, y, z_{1,1}, \dots, z_{m,q}) \left| \begin{array}{l} x_{i,\ell} \mapsto \sum_{j=1}^q \omega^{-\text{tr}(\alpha_\ell \alpha_j)} x_{i,j}, \\ y \mapsto \frac{1-y}{1+(q-1)y}, \\ z_{i,\ell} \mapsto \sum_{j=1}^q \omega^{-\text{tr}(\alpha_\ell \alpha_j)} z_{i,j} \end{array} \right. \\
W_{\widehat{\mathcal{C}}_{(j)}}(x_{1,1}, \dots, x_{m,q}, y, z_{1,1}, \dots, z_{m,q}) &= \frac{(1 + (q-1)y)^n}{q^{m+k}} W_{\mathcal{C}_{(j)}}(x_{1,1}, \dots, x_{m,q}, y, z_{1,1}, \dots, z_{m,q}) \left| \begin{array}{l} x_{i,\ell} \mapsto \sum_{j=1}^q \omega^{-\text{tr}(\alpha_\ell \alpha_j)} x_{i,j}, \\ y \mapsto \frac{1-y}{1+(q-1)y}, \\ z_{i,\ell} \mapsto \sum_{j=1}^q \omega^{+\text{tr}(\alpha_\ell \alpha_j)} z_{i,j} \end{array} \right.
\end{aligned}$$

□

If  $\mathcal{C}_{(j)}$  is systematic, the above result can be extended to the input-parity weight enumerator by further splitting the weights for  $\mathbf{p}_j$  (or equivalently  $\mathbf{v}_2$ ) as a two-split in  $y_I$  and  $y_P$  for inputs and parities. In other words, say  $\mathbf{v}_2 = (\mathbf{v}_{2,I}^\top : \mathbf{v}_{2,P}^\top)^\top$  and redefine the weight function as

$$f_{\text{IP}}(\mathbf{v}_1, \mathbf{v}_{2,I}, \mathbf{v}_{2,P}, \mathbf{v}_3) = \left[ \prod_{i=1}^m \prod_{j=1}^q x_{i,j}^{\text{wt}_j(v_{1,i})} \right] y_I^{\text{wt}(\mathbf{v}_{2,I})} y_P^{\text{wt}(\mathbf{v}_{2,P})} \left[ \prod_{i=1}^m \prod_{j=1}^q z_{i,j}^{\text{wt}_j(v_{3,i})} \right]$$

Then the following corollary is immediate.

**Corollary 30.** The input-parity weight enumerator for  $\widehat{\mathcal{C}}_{(j)}$  is

$$\begin{aligned}
W_{\widehat{\mathcal{C}}_{(j)}}(x_{1,1}, \dots, x_{m,q}, y_I, y_P, z_{1,1}, \dots, z_{m,q}) &= \frac{(1 + (q-1)y_I)^k (1 + (q-1)y_P)^{n-k}}{q^{m+k}} \\
&\times W_{\mathcal{C}_{(j)}}(x_{1,1}, \dots, x_{m,q}, y_I, y_P, z_{1,1}, \dots, z_{m,q}) \left| \begin{array}{l} x_{i,\ell} \mapsto \sum_{j=1}^q \omega^{-\text{tr}(\alpha_\ell \alpha_j)} x_{i,j}, \\ y_I \mapsto \frac{1-y_I}{1+(q-1)y_I}, \\ y_P \mapsto \frac{1-y_P}{1+(q-1)y_P}, \\ z_{i,\ell} \mapsto \sum_{j=1}^q \omega^{\text{tr}(\alpha_\ell \alpha_j)} z_{i,j} \end{array} \right.
\end{aligned}$$

□

### B. Enumerate in Matrix: Weight Adjacency Matrix

We may also enumerate the codewords in  $\mathcal{C}_{(j)}$  in a matrix form. To this end, we index the entries of a matrix  $A \in \mathbf{M}_{q^m}(\mathbb{Z}[y])$  by  $(\mathbf{v}_1, \mathbf{v}_3) \in \mathbb{F}_q^m \times \mathbb{F}_q^m$ . Let  $\mathbf{e}_{\mathbf{v}} \in \{0, 1\}^{q^m}$  be a length- $q^m$  vector in  $\mathbb{R}^{q^m}$  such that  $(\mathbf{e}_{\mathbf{v}})_i = 1$  if the index  $i$  is associated with vector  $\mathbf{v} \in \mathbb{F}_q^m$ , and  $(\mathbf{e}_{\mathbf{v}})_i = 0$  if otherwise. With the above, for any  $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) \in \mathbb{F}_q^m \times \mathbb{F}_q^n \times \mathbb{F}_q^m$ , we consider the following weight function

$$f_{\text{mat}}(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) = y^{\text{wt}(\mathbf{v}_2)} \mathbf{e}_{\mathbf{v}_1}^\top \mathbf{e}_{\mathbf{v}_3}.$$

**Definition 31.** The weight adjacency matrix for  $\mathcal{C}_{(j)}$  is the weight enumerator for  $\mathcal{C}_{(j)}$  based on weight function  $f_{\text{mat}}$ , i.e.,

$$\Lambda_{\mathcal{C}_{(j)}}(y) = \sum_{(\mathbf{w}_j^\top : \mathbf{p}_j^\top : \mathbf{w}_{j+1}^\top)^\top \in \mathcal{C}_{(j)}} f_{\text{mat}}(\mathbf{w}_j, \mathbf{p}_j, \mathbf{w}_{j+1}).$$

□

The Fourier transform of  $f_{\text{mat}}$  over  $\mathcal{V}$  with respect to kernel  $\chi_{\mathbf{u}}(\mathbf{v})$  is given by

$$\begin{aligned}
F_{\text{mat}}(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3) &= \sum_{(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) \in \mathcal{V}} y^{\text{wt}(\mathbf{v}_2)} \mathbf{e}_{\mathbf{v}_1}^\top \mathbf{e}_{\mathbf{v}_3} \omega^{-\sum_{i=1}^3 \text{tr}(\mathbf{u}_i^\top \mathbf{v}_i)} \\
&= \left( \sum_{\mathbf{v}_1 \in \mathbb{F}_q^m} \omega^{-\text{tr}(\mathbf{u}_1^\top \mathbf{v}_1)} \mathbf{e}_{\mathbf{v}_1}^\top \right) \left[ \sum_{\mathbf{v}_2 \in \mathbb{F}_q^n} y^{\text{wt}(\mathbf{v}_2)} \omega^{-\text{tr}(\mathbf{u}_2^\top \mathbf{v}_2)} \right] \left( \sum_{\mathbf{v}_3 \in \mathbb{F}_q^m} \omega^{-\text{tr}(\mathbf{u}_3^\top \mathbf{v}_3)} \mathbf{e}_{\mathbf{v}_3}^\top \right)
\end{aligned} \tag{23}$$

In particular, let  $\mathfrak{F}_{q^m}$  be the standard  $q^m$ -point FFT matrix given by

$$\mathfrak{F}_{q^m} := \sum_{\mathbf{u} \in \mathbb{F}_q^m} \sum_{\mathbf{v} \in \mathbb{F}_q^m} \omega^{-\text{tr}(\mathbf{u}^\top \mathbf{v})} \mathbf{e}_{\mathbf{v}} \mathbf{e}_{\mathbf{u}}^\top;$$

then (23) can be rewritten as

$$F_{\text{mat}}(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3) = (1 + (q-1)y)^{n-\text{wt}(\mathbf{u}_2)} (1-y)^{\text{wt}(\mathbf{u}_2)} \mathfrak{F}_{q^m} \mathbf{e}_{\mathbf{u}_1} \mathbf{e}_{\mathbf{u}_3}^\top \mathfrak{F}_{q^m}^\top.$$

Substituting the above into (22) yields the following result.

**Theorem 32.** The weight adjacency matrices for  $\mathcal{C}_{(j)}^\perp$  and  $\widehat{\mathcal{C}}_{(j)}$  are given respectively by

$$\begin{aligned} \Lambda_{\mathcal{C}_{(j)}^\perp}(y) &= \frac{(1 + (q-1)y)^n}{q^{m+k}} \mathfrak{F}_{q^m} \Lambda_{\mathcal{C}_{(j)}} \left( \frac{1-y}{1 + (q-1)y} \right) \mathfrak{F}_{q^m}^\top \\ \Lambda_{\widehat{\mathcal{C}}_{(j)}}(y) &= \frac{(1 + (q-1)y)^n}{q^{m+k}} \mathfrak{F}_{q^m} \Lambda_{\mathcal{C}_{(j)}} \left( \frac{1-y}{1 + (q-1)y} \right) \mathfrak{F}_{q^m}^\dagger \end{aligned}$$

□

Same as before, when  $\mathcal{C}_{(j)}$  is systematic, we can split the weights of  $\mathbf{v}_2$  to formulate the following weight function

$$f_{\text{mat,IP}}(\mathbf{v}_1, \mathbf{v}_{2,I}, \mathbf{v}_{2,P}, \mathbf{v}_3) = y_I^{\text{wt}(\mathbf{v}_{2,I})} y_P^{\text{wt}(\mathbf{v}_{2,P})} \mathbf{e}_{\mathbf{v}_1} \mathbf{e}_{\mathbf{v}_3}^\top.$$

This leads to the following duality for input-parity weight enumerators.

**Corollary 33.**

$$\begin{aligned} \Lambda_{\mathcal{C}_{(j)}^\perp}(y_I, y_P) &= \frac{(1 + (q-1)y_I)^k (1 + (q-1)y_P)^{n-k}}{q^{m+k}} \mathfrak{F}_{q^m} \Lambda_{\mathcal{C}_{(j)}} \left( \frac{1-y_I}{1 + (q-1)y_I}, \frac{1-y_P}{1 + (q-1)y_P} \right) \mathfrak{F}_{q^m}^\top, \\ \Lambda_{\widehat{\mathcal{C}}_{(j)}}(y_I, y_P) &= \frac{(1 + (q-1)y_I)^k (1 + (q-1)y_P)^{n-k}}{q^{m+k}} \mathfrak{F}_{q^m} \Lambda_{\mathcal{C}_{(j)}} \left( \frac{1-y_I}{1 + (q-1)y_I}, \frac{1-y_P}{1 + (q-1)y_P} \right) \mathfrak{F}_{q^m}^\dagger. \end{aligned}$$

□

## APPENDIX B

### THE POLYNOMIAL CHECK MATRIX OF AN EAQ CONVOLUTIONAL CODE

In the case of the quotient Pauli group  $\bar{\mathcal{G}}_1 = \langle [I], [X], [Y], [Z] \rangle$  (in order), which is isomorphic to  $\mathbb{Z}_2^2$ . Define a map  $\phi : \bar{\mathcal{G}}_1 \rightarrow \mathbb{Z}_2^2$  by

$$\begin{aligned} I &\mapsto 00 \\ X &\mapsto 01 \\ Z &\mapsto 10 \\ Y &\mapsto 11. \end{aligned}$$

Thus an induced map  $\phi^n : \bar{\mathcal{G}}_n \rightarrow \mathbb{Z}_2^{2n}$  can be defined naturally by

$$\phi^n(E_1 \otimes \cdots \otimes E_n) = \phi(E_1) : \cdots : \phi(E_n).^7$$

Sometimes we omit the superscript  $n$  of  $\phi^n$  when it is clear from the context. There exists a  $2n \times 2n$  matrix  $M_U = (\phi(UZ_1U^\dagger)^T \phi(UX_1U^\dagger)^T \cdots \phi(UZ_nU^\dagger)^T \phi(UX_nU^\dagger)^T)$  so that applying a unitary operator  $U$  on a Pauli operator  $E$  corresponds to multiplying  $\phi(E)$  by  $M_U$ .

Suppose  $U$  is the seed transformation corresponding to an  $((n, k, c, m))$  EA-QCC. Let

$$M_U = \begin{pmatrix} \overbrace{F}^{2n} & \overbrace{A}^{2m} \\ G & B \\ H & C \\ K & E \end{pmatrix} \begin{matrix} \} 2m \\ \} 2k \\ \} 2(n-k-c) \\ \} 2c \end{matrix},$$

<sup>7</sup>For our purpose this definition of binary  $2n$ -tuple is different from the usual one: the first and the second halves are corresponding to  $Z$  and  $X$  operators, respectively.

where the submatrices have the corresponding dimensions. We have

$$\begin{aligned} & \phi^n(P_i) : \phi^m(M_{i+1}) \\ &= \phi^m(M_i) : \phi^k(L_i) : \phi^{n-k-c}(S_i^Z) : \phi^c(S_i^E) \begin{pmatrix} F & A \\ G & B \\ H & C \\ K & E \end{pmatrix}. \end{aligned}$$

Let  $S^Z(D)$  be the  $n-k-c \times 2n$  polynomial matrix so that its  $i$ -th row is the binary representation of the impulse response of  $I^{\otimes m} \otimes I^{\otimes k} \otimes Z_i \otimes I^{\otimes c}$  for  $Z_i \in \{I, Z\}^{\otimes n-k-c}$ , that is,

$$\phi(\mathcal{U}_E(I^{\otimes m} \otimes I^{\otimes k} \otimes Z_i \otimes I^{\otimes c})\mathcal{U}_E^\dagger),$$

where  $\mathcal{U}_E = \prod_j D^{j-1}[U_{(j)}]$  is the encoding operator of the EA-QCC. Then

$$\begin{aligned} S^Z(D) &= \sum_{i=0}^{\infty} D^i P_i = H^Z + DC^Z \sum_{i=0}^{\infty} (DA)^i F \\ &= H^Z + DC^Z (I - DA)^{-1} F, \end{aligned}$$

where  $H^Z = (I_{n-k-c} \otimes [1 \ 0])H$  and  $C^Z = (I_c \otimes [1 \ 0])C$ . (Note that  $I_c$  is the  $c \times c$  identity matrix.) This equation parallels the classical equation (7). Now let  $S^E(D)$  be the  $c \times 2n$  polynomial matrix so that its  $2i-1$  and  $2i$ -th row are the binary representations of the impulse response of  $I^{\otimes m} \otimes I^{\otimes k} \otimes I^{\otimes n-k-c} \otimes Z_i$  and  $I^{\otimes m} \otimes I^{\otimes k} \otimes I^{\otimes n-k-c} \otimes X_i$  for  $Z_i \in \{I, Z\}^{\otimes n-k-c}$  and  $X_i \in \{I, Z\}^{\otimes n-k-c}$ , respectively. Similarly, we have

$$S^E(D) = K + DE(I - DA)^{-1} F.$$

As a consequence, the  $n-k \times 2n$  polynomial matrix

$$S(D) = \begin{pmatrix} S^Z(D) \\ S^E(D) \end{pmatrix}$$

defines the simplified stabilizer matrix for the EA-QCC. When  $c = 0$ ,  $S(D)$  is the stabilizer matrix for QCC used in [22], [23], [24], [25] up to a permutation of the columns.

One can also obtain the polynomial matrix  $L(D)$  for the impulse response of the logical operators in the same way and

$$L(D) = G + DB(I - DA)^{-1} F.$$

The orthogonality of  $L(D)$  and  $S(D)$  follows directly from the definition. To sum up, we have

$$\begin{pmatrix} L(D) \\ S^Z(D) \\ S^E(D) \end{pmatrix} = \begin{pmatrix} G \\ H^Z \\ K \end{pmatrix} + D \begin{pmatrix} B \\ C^Z \\ E \end{pmatrix} (I - DA)^{-1} F.$$

## REFERENCES

- [1] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.
- [2] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes," accessed on 2010-12-01. [Online]. Available: <http://www.codetables.de/>
- [3] J. Forney, G.D., "Convolutional codes i: Algebraic structure," *IEEE Trans. Inf. Theory*, vol. 16, no. 6, pp. 720–738, Nov 1970.
- [4] A. Viterbi, "Convolutional codes and their performance in communication systems," *IEEE Trans. Com. Tech.*, vol. 19, no. 5, pp. 751–772, October 1971.
- [5] J. B. Shearer and R. J. McEliece, "There is no MacWilliams identity for convolutional codes," *IEEE Trans. Inf. Theory*, vol. IT-23, no. 6, pp. 775–776, 1977.
- [6] J. Massey and M. Sain, "Codes, automata, and continuous systems: Explicit interconnections," *Automatic Control, IEEE Transactions on*, vol. 12, no. 6, pp. 644–650, December 1967.
- [7] K. Abdel-Ghaffar, "On unit constraint-length convolutional codes," *IEEE Trans. Inf. Theory*, vol. 38, no. 1, pp. 200–206, Jan 1992.
- [8] R. J. McEliece, *The Theory of Information and Coding*. Cambridge University Press, 2002.
- [9] H. Gluesing-Luerssen, "On the weight distribution of convolutional codes," *Linear Algebra and its Applications*, vol. 408, pp. 298–326, 2005.
- [10] H. Gluesing-Luerssen and G. Schneider, "On the MacWilliams identity for convolutional codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 4, pp. 1536–1550, 2008.
- [11] —, "A MacWilliams identity for convolutional codes: The general case," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 2920–2930, 2009.
- [12] J. Forney, G.D., "Codes on graphs: normal realizations," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 520–548, 2001.
- [13] —, "Codes on graphs: Duality and MacWilliams identities," *IEEE Trans. Inf. Theory*, vol. 57, no. 3, pp. 1382–1397, 2011.
- [14] P. Shor and R. Laflamme, "Quantum analog of the MacWilliams identities for classical coding theory," *Phys. Rev. Lett.*, vol. 78, no. 8, pp. 1600–1602, Feb 1997.
- [15] E. M. Rains, "Quantum weight enumerators," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1388 – 1394, 1995.
- [16] A. Ashikhmin and S. Litsyn, "Upper bounds on the size of quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1206 – 1215, 1999.
- [17] C.-Y. Lai, T. A. Brun, and M. M. Wilde, "Duality in entanglement-assisted quantum error correction," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 4020–4024, 2013.
- [18] D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. dissertation, California Institute of Technology, Pasadena, CA, 1997. [Online]. Available: <http://arxiv.org/abs/quant-ph/9705052>

- [19] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, UK: Cambridge University Press, 2000.
- [20] T. A. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, pp. 436–439, 2006.
- [21] T. Brun, I. Devetak, and M.-H. Hsieh, "Catalytic quantum error correction," 2006. [Online]. Available: <http://arxiv.org/abs/quant-ph/0608027>
- [22] H. Ollivier and J.-P. Tillich, "Description of a quantum convolutional code," *Phys. Rev. Lett.*, vol. 91, p. 177902, Oct 2003. [Online]. Available: <http://link.aps.org/doi/10.1103/PhysRevLett.91.177902>
- [23] G. Forney, M. Grassl, and S. Guha, "Convolutional and tail-biting quantum error-correcting codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 865–880, 2007.
- [24] M. Grassl and M. Rotteler, "Non-catastrophic encoders and encoder inverses for quantum convolutional codes," in *Proc. 2006 IEEE Intl. Symp. Inf. Theory.*, 2006, pp. 1109–1113.
- [25] —, "Constructions of quantum convolutional codes," in *Proc. 2007 IEEE Intl. Symp. Inf. Theory*, 2007, pp. 816–820.
- [26] M. M. Wilde, "Quantum-shift-register circuits," *Phys. Rev. A*, vol. 79, p. 062325, Jun 2009. [Online]. Available: <http://link.aps.org/doi/10.1103/PhysRevA.79.062325>
- [27] D. Poulin, J.-P. Tillich, and H. Ollivier, "Quantum serial turbo codes," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2776–2798, 2009.
- [28] M. M. Wilde and M.-H. Hsieh, "Entanglement boosts quantum turbo codes," in *Proc. 2011 IEEE Intl. Symp. Inf. Theory*, 2011, pp. 445–449.
- [29] M. M. Wilde, M.-H. Hsieh, and Z. Babar, "Entanglement-assisted quantum turbo codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 1203–1222, 2014.
- [30] M. M. Wilde and T. A. Brun, "Extra shared entanglement reduces memory demand in quantum convolutional coding," *Phys. Rev. A*, vol. 79, p. 032313, Mar 2009. [Online]. Available: <http://link.aps.org/doi/10.1103/PhysRevA.79.032313>
- [31] —, "Entanglement-assisted quantum convolutional coding," *Phys. Rev. A*, vol. 81, p. 042333, Apr 2010. [Online]. Available: <http://link.aps.org/doi/10.1103/PhysRevA.81.042333>
- [32] —, "Quantum convolutional coding with shared entanglement: general structure," *Quant. Inf. Proc.*, vol. 9, no. 5, pp. 509–540, 2010. [Online]. Available: <http://dx.doi.org/10.1007/s11128-010-0179-9>
- [33] Y. Mao and F. Kschischang, "On factor graphs and the Fourier transform," *IEEE Trans. Inf. Theory*, vol. 51, no. 5, pp. 1635–1649, 2005.
- [34] A. Al-Bashabsheh and Y. Mao, "Normal factor graphs and holographic transformations," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 752–763, 2011.
- [35] J. Forney, G.D., "Structural analysis of convolutional codes via dual codes," *Information Theory, IEEE Transactions on*, vol. 19, no. 4, pp. 512–518, Jul 1973.
- [36] H.-F. Lu, P. Kumar, and E. hui Yang, "On the input-output weight enumerators of product accumulate codes," *IEEE Communications Letters*, vol. 8, no. 8, pp. 520–522, Aug 2004.
- [37] M.-C. Chiu and H.-F. Lu, "Accumulate codes based on 1+D convolutional outer codes," *Communications, IEEE Transactions on*, vol. 57, no. 2, pp. 311–314, February 2009.
- [38] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over  $GF(4)$ ," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, 1998. [Online]. Available: <http://arxiv.org/abs/quant-ph/9608006>
- [39] C.-Y. Lai and T. A. Brun, "Entanglement-assisted quantum error-correcting codes with imperfect ebits," *Phys. Rev. A*, vol. 86, p. 032319, Sep 2012. [Online]. Available: <http://link.aps.org/doi/10.1103/PhysRevA.86.032319>
- [40] —, "Entanglement increases the error-correcting ability of quantum error-correcting codes," *Phys. Rev. A*, vol. 88, p. 012320, Jul 2013. [Online]. Available: <http://link.aps.org/doi/10.1103/PhysRevA.88.012320>
- [41] C.-Y. Lai, T. A. Brun, and M. M. Wilde, "Dualities and identities for entanglement-assisted quantum codes," *Quant. Inf. Proc.*, pp. 1–34, 2013. [Online]. Available: <http://dx.doi.org/10.1007/s11128-013-0704-8>
- [42] I. Bocharova, F. Hug, R. Johannesson, and B. Kudryashov, "Dual convolutional codes and the macwilliams identities," *Problems of Information Transmission*, vol. 48, no. 1, pp. 21–30, 2012. [Online]. Available: <http://dx.doi.org/10.1134/S0032946012010036>
- [43] I. Kremsky, M.-H. Hsieh, and T. A. Brun, "Classical enhancement of quantum error-correcting codes," *Phys. Rev. A*, vol. 78, p. 012341, 2008.
- [44] M.-H. Hsieh, I. Devetak, and T. A. Brun, "General entanglement-assisted quantum error-correcting codes," *Phys. Rev. A*, vol. 76, p. 062313, 2007.